

TigerSwitch 10/100

24-Port Fast Ethernet Switch

- ◆ 24 10BASE-T/100BASE-TX auto MDI/MDI-X ports
- ◆ Optional 1000BASE-X or 100BASE-FX modules
- ◆ 8.8 Gbps of aggregate bandwidth
- ◆ Non-blocking switching architecture
- ◆ Spanning Tree Protocol
- ◆ Up to four port trunks
- ◆ RADIUS authentication
- ◆ Rate limiting for bandwidth management
- ◆ QoS support for four-level priority
- ◆ Full support for VLANs with GVRP
- ◆ IP Multicasting with IGMP Snooping
- ◆ Manageable via console, Web, SNMP/RMON



TigerSwitch 10/100 Management Guide

From SMC's Tiger line of feature-rich workgroup LAN solutions



38 Tesla
Irvine, CA 92618
Phone: (949) 679-8000

May 2003
Pub. # 150200033600A

Information furnished by SMC Networks, Inc. (SMC) is believed to be accurate and reliable. However, no responsibility is assumed by SMC for its use, nor for any infringements of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of SMC. SMC reserves the right to change specifications at any time without notice.

Copyright © 2003 by
SMC Networks, Inc.
38 Tesla
Irvine, CA 92618
All rights reserved. Printed in Taiwan

Trademarks:

SMC is a registered trademark; and EZ Switch, TigerStack and TigerSwitch are trademarks of SMC Networks, Inc. Other product and company names are trademarks or registered trademarks of their respective holders.

LIMITED WARRANTY

Limited Warranty Statement: SMC Networks, Inc. ("SMC") warrants its products to be free from defects in workmanship and materials, under normal use and service, for the applicable warranty term. All SMC products carry a standard 90-day limited warranty from the date of purchase from SMC or its Authorized Reseller. SMC may, at its own discretion, repair or replace any product not operating as warranted with a similar or functionally equivalent product, during the applicable warranty term. SMC will endeavor to repair or replace any product returned under warranty within 30 days of receipt of the product.

The standard limited warranty can be upgraded to a Limited Lifetime* warranty by registering new products within 30 days of purchase from SMC or its Authorized Reseller. Registration can be accomplished via the enclosed product registration card or online via the SMC web site. Failure to register will not affect the standard limited warranty. The Limited Lifetime warranty covers a product during the Life of that Product, which is defined as the period of time during which the product is an "Active" SMC product. A product is considered to be "Active" while it is listed on the current SMC price list. As new technologies emerge, older technologies become obsolete and SMC will, at its discretion, replace an older product in its product line with one that incorporates these newer technologies. At that point, the obsolete product is discontinued and is no longer an "Active" SMC product. A list of discontinued products with their respective dates of discontinuance can be found at:

http://www.smc.com/index.cfm?action=customer_service_warranty.

All products that are replaced become the property of SMC. Replacement products may be either new or reconditioned. Any replaced or repaired product carries either a 30-day limited warranty or the remainder of the initial warranty, whichever is longer. SMC is not responsible for any custom software or firmware, configuration information, or memory data of Customer contained in, stored on, or integrated with any products returned to SMC pursuant to any warranty. Products returned to SMC should have any customer-installed accessory or add-on components, such as expansion modules, removed prior to returning the product for replacement. SMC is not responsible for these items if they are returned with the product.

Customers must contact SMC for a Return Material Authorization number prior to returning any product to SMC. Proof of purchase may be required. Any product returned to SMC without a valid Return Material Authorization (RMA) number clearly marked on the outside of the package will be returned to customer at customer's expense. For warranty claims within North America, please call our toll-free customer support number at (800) 762-4968. Customers are responsible for all shipping charges from their facility to SMC. SMC is responsible for return shipping charges from SMC to customer.

WARRANTIES EXCLUSIVE: IF AN SMC PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER'S SOLE REMEDY SHALL BE REPAIR OR REPLACEMENT OF THE PRODUCT IN QUESTION, AT SMC'S OPTION. THE

LIMITED WARRANTY

FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OR CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. SMC NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS. SMC SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLIGENCE, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

LIMITATION OF LIABILITY: IN NO EVENT, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), SHALL SMC BE LIABLE FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE, LOSS OF BUSINESS, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF SMC OR ITS AUTHORIZED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR THE LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES FOR CONSUMER PRODUCTS, SO THE ABOVE LIMITATIONS AND EXCLUSIONS MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, WHICH MAY VARY FROM STATE TO STATE. NOTHING IN THIS WARRANTY SHALL BE TAKEN TO AFFECT YOUR STATUTORY RIGHTS.

* SMC will provide warranty service for one year following discontinuance from the active SMC price list. Under the limited lifetime warranty, internal and external power supplies, fans, and cables are covered by a standard one-year warranty from date of purchase.

SMC Networks, Inc.
38 Tesla
Irvine, CA 92618

CONTENTS

| | | |
|----------|--|------------|
| 1 | Switch Management | 1-1 |
| | Connecting to the Switch | 1-1 |
| | Configuration Options | 1-1 |
| | Required Connections | 1-3 |
| | Remote Connections | 1-4 |
| | Basic Configuration | 1-5 |
| | Console Connection | 1-5 |
| | Setting Passwords | 1-6 |
| | Setting an IP Address | 1-7 |
| | Enabling SNMP Management Access | 1-10 |
| | Saving Configuration Settings | 1-12 |
| | Managing System Files | 1-13 |
| | System Defaults | 1-14 |
| | | |
| 2 | Configuring the Switch | 2-1 |
| | Using the Web Interface | 2-1 |
| | Navigating the Web Browser Interface | 2-2 |
| | Home Page | 2-3 |
| | Configuration Options | 2-3 |
| | Panel Display | 2-4 |
| | Main Menu | 2-5 |
| | Basic Configuration | 2-9 |
| | Displaying System Information | 2-9 |
| | Setting the IP Address | 2-11 |
| | Configuring User Authentication | 2-15 |
| | Configuring the Logon Password | 2-15 |
| | Configuring RADIUS Logon Authentication | 2-17 |
| | Managing Firmware | 2-20 |
| | Downloading System Software from a Server | 2-20 |
| | Saving or Restoring Configuration Settings | 2-22 |
| | Resetting the System | 2-24 |
| | Displaying Bridge Extension Capabilities | 2-24 |
| | Enabling or Disabling GVRP | |
| | (Global Setting) | 2-27 |
| | Displaying Switch Hardware/Software Versions | 2-28 |

| | |
|---|------|
| Port Configuration | 2-30 |
| Displaying Connection Status | 2-30 |
| Configuring Interface Connections | 2-32 |
| Setting Broadcast Storm Thresholds | 2-34 |
| Configuring Port Mirroring | 2-37 |
| Address Table Settings | 2-38 |
| Setting Static Addresses | 2-39 |
| Displaying the Address Table | 2-40 |
| Changing the Aging Time | 2-42 |
| Spanning Tree Algorithm Configuration | 2-42 |
| Managing Global Settings | 2-43 |
| Displaying the Global Settings for STA | 2-45 |
| Configuring the Global Settings for STA | 2-47 |
| Managing STA Interface Settings | 2-47 |
| Displaying the Interface Settings for STA | 2-51 |
| Configuring the Interface Settings for STA | 2-52 |
| VLAN Configuration | 2-52 |
| Displaying Basic VLAN Information | 2-56 |
| Displaying Current VLANs | 2-57 |
| Creating VLANs | 2-59 |
| Adding Static Members to VLANs (VLAN Index) | 2-61 |
| Adding Static Members to VLANs (Port Index) | 2-64 |
| Configuring VLAN Behavior for Interfaces | 2-65 |
| Configuring Private VLANs | 2-68 |
| Displaying Current Private VLANs | 2-69 |
| Configuring Private VLANs | 2-71 |
| Associating Community VLANs | 2-72 |
| Displaying Private VLAN Interface Information | 2-73 |
| Configuring Private VLAN Interfaces | 2-75 |
| Class of Service Configuration | 2-77 |
| Setting the Queue Mode | 2-78 |
| Port Trunk Configuration | 2-79 |
| Configuring SNMP | 2-82 |
| Setting Community Access Strings | 2-83 |
| Specifying Trap Managers and Trap Types | 2-84 |
| Multicast Configuration | 2-86 |
| Configuring IGMP Parameters | 2-87 |

| | |
|--|-------|
| Interfaces Attached to a Multicast Router | 2-89 |
| Specifying Interfaces Attached to a Multicast Router . . . | 2-91 |
| Displaying Port Members of Multicast Services | 2-92 |
| Adding Multicast Addresses to VLANs | 2-94 |
| Showing Port Statistics | 2-96 |
| Rate Limit Configuration | 2-98 |
| Configuring 802.1x Port Authentication | 2-100 |
| Displaying 802.1x Global Settings | 2-102 |
| Configuring 802.1x Global Settings | 2-103 |
| Configuring a Port for Authorization | 2-105 |
| Displaying 802.1x Statistics | 2-107 |

3 Command Line Interface 3-1

| | |
|--|------|
| Using the Command Line Interface | 3-1 |
| Accessing the CLI | 3-1 |
| Console Connection | 3-1 |
| Telnet Connection | 3-2 |
| Entering Commands | 3-4 |
| Keywords and Arguments | 3-4 |
| Minimum Abbreviation | 3-4 |
| Command Completion | 3-5 |
| Getting Help on Commands | 3-5 |
| Partial Keyword Lookup | 3-6 |
| Negating the Effect of Commands | 3-6 |
| Using Command History | 3-6 |
| Understanding Command Modes | 3-7 |
| Exec Commands | 3-7 |
| Configuration Commands | 3-8 |
| Command Line Processing | 3-10 |
| Command Groups | 3-10 |
| General Commands | 3-13 |
| enable | 3-13 |
| disable | 3-14 |
| configure | 3-15 |
| show history | 3-16 |
| reload | 3-17 |
| end | 3-17 |

| | |
|------------------------------|------|
| exit | 3-18 |
| quit | 3-19 |
| Flash/File Commands | 3-19 |
| copy | 3-20 |
| delete | 3-22 |
| dir | 3-23 |
| whichboot | 3-24 |
| boot system | 3-25 |
| System Management Commands | 3-26 |
| hostname | 3-27 |
| username | 3-27 |
| enable password | 3-29 |
| ip http port | 3-30 |
| ip http server | 3-31 |
| show startup-config | 3-32 |
| show running-config | 3-34 |
| show system | 3-36 |
| show users | 3-37 |
| show version | 3-37 |
| Authentication Commands | 3-38 |
| authentication login | 3-39 |
| radius-server host | 3-40 |
| radius-server port | 3-41 |
| radius-server key | 3-42 |
| radius-server retransmit | 3-42 |
| radius-server timeout | 3-43 |
| show radius-server | 3-43 |
| Port Authentication Commands | 3-44 |
| authentication dot1x | 3-45 |
| dot1x default | 3-46 |
| dot1x max-req | 3-46 |
| dot1x port-control | 3-47 |
| dot1x re-authenticate | 3-48 |
| dot1x re-authentication | 3-48 |
| dot1x timeout quiet-period | 3-49 |
| dot1x timeout re-authperiod | 3-49 |
| dot1x timeout tx-period | 3-50 |

| | |
|--|------|
| show dot1x | 3-51 |
| SNMP Commands | 3-54 |
| snmp-server community | 3-54 |
| snmp-server contact | 3-55 |
| snmp-server location | 3-56 |
| snmp-server host | 3-57 |
| snmp-server enable traps | 3-58 |
| show snmp | 3-59 |
| IGMP Snooping Commands | 3-61 |
| ip igmp snooping | 3-61 |
| ip igmp snooping query-count | 3-62 |
| ip igmp snooping query-max-response-time | 3-63 |
| ip igmp snooping router-port-expire-time | 3-64 |
| ip igmp snooping version | 3-65 |
| show ip igmp snooping | 3-66 |
| show mac-address-table multicast | 3-67 |
| Line Commands | 3-68 |
| line | 3-69 |
| login | 3-70 |
| password | 3-71 |
| exec-timeout | 3-72 |
| password-thresh | 3-73 |
| silent-time | 3-74 |
| databits | 3-75 |
| parity | 3-76 |
| speed | 3-77 |
| stopbits | 3-78 |
| show line | 3-78 |
| IP Commands | 3-79 |
| ip address | 3-80 |
| ip dhcp restart | 3-81 |
| ip default-gateway | 3-82 |
| show ip interface | 3-83 |
| show ip redirects | 3-84 |
| ping | 3-84 |
| HOL Blocking Prevention Commands | 3-86 |
| queue hol-prevention | 3-86 |

| | |
|---|-------|
| show queue hol-prevention | 3-87 |
| Interface Commands | 3-88 |
| interface | 3-89 |
| description | 3-90 |
| speed-duplex | 3-90 |
| negotiation | 3-92 |
| capabilities | 3-93 |
| flowcontrol | 3-94 |
| shutdown | 3-96 |
| switchport broadcast percent | 3-97 |
| clear counters | 3-98 |
| show interfaces status | 3-99 |
| show interfaces counters | 3-100 |
| show interfaces switchport | 3-102 |
| Rate Limit Commands | 3-104 |
| rate-limit | 3-105 |
| Address Table Commands | 3-106 |
| mac-address-table static | 3-107 |
| clear mac-address-table dynamic | 3-108 |
| show mac-address-table | 3-109 |
| mac-address-table aging-time | 3-110 |
| show mac-address-table aging-time | 3-111 |
| Spanning Tree Commands | 3-111 |
| spanning-tree | 3-112 |
| spanning-tree forward-time | 3-113 |
| spanning-tree hello-time | 3-114 |
| spanning-tree max-age | 3-115 |
| spanning-tree priority | 3-116 |
| spanning-tree cost | 3-116 |
| spanning-tree port-priority | 3-117 |
| spanning-tree portfast | 3-118 |
| show spanning-tree | 3-119 |
| VLAN Commands | 3-121 |
| vlan database | 3-122 |
| vlan | 3-123 |
| interface vlan | 3-124 |
| switchport mode | 3-125 |

| | |
|--|-------|
| switchport acceptable-frame-types | 3-126 |
| switchport ingress-filtering | 3-127 |
| switchport native vlan | 3-128 |
| switchport allowed vlan | 3-129 |
| switchport forbidden vlan | 3-130 |
| show vlan | 3-131 |
| Private VLAN Commands | 3-132 |
| private-vlan | 3-134 |
| private vlan association | 3-135 |
| switchport mode private-vlan | 3-136 |
| switchport private-vlan host-association | 3-137 |
| switchport private-vlan mapping | 3-138 |
| show vlan private-vlan | 3-139 |
| GVRP and Bridge Extension Commands | 3-140 |
| switchport gvrp | 3-140 |
| show gvrp configuration | 3-141 |
| garp timer | 3-142 |
| show garp timer | 3-143 |
| bridge-ext gvrp | 3-144 |
| show bridge-ext | 3-145 |
| Priority Commands | 3-146 |
| queue mode | 3-147 |
| show queue mode | 3-147 |
| Mirror Port Commands | 3-148 |
| port monitor | 3-148 |
| show port monitor | 3-149 |
| Port Trunking Commands | 3-150 |
| port-group | 3-152 |

A TroubleshootingA-1
Troubleshooting Chart A-1

B Upgrading Firmware via the Serial PortB-1
Restoring Switch Defaults B-4

C Pin AssignmentsC-1
Console Port Pin Assignments C-1
 DB-9 Port Pin Assignments C-2
 Console Port to 9-Pin DTE Port on PC C-2
 Console Port to 25-Pin DTE Port on PC C-2

Glossary

Index

CHAPTER 1

SWITCH MANAGEMENT

Connecting to the Switch

Configuration Options

This switch includes a built-in network management agent. The agent offers a variety of management options, including SNMP, RMON and a Web-based interface. A PC may also be connected directly to the switch for configuration and monitoring via a command line interface (CLI).

Note: The IP address for this switch is unassigned by default. To change this address, see “Setting an IP Address” on page 1-7.

The switch’s HTTP Web agent allows you to configure switch parameters, monitor port connections, and display statistics using a standard Web browser such as Netscape Navigator version 6.2 and higher or Microsoft IE version 5.0 and higher. The switch’s Web management interface can be accessed from any computer attached to the network.

The switch’s management agent is based on SNMP (Simple Network Management Protocol). This SNMP agent permits the switch to be managed from any system in the network using the appropriate management software.

The CLI program can be accessed by a direct connection to the RS-232 serial console port on the switch, or remotely by a Telnet connection over the network.

The switch's CLI configuration program, Web interface, and SNMP agent allow you to perform the following management functions:

- Set user names and passwords for up to 16 users
- Set an IP interface for a management VLAN
- Configure SNMP parameters and enable traps
- Enable/disable any port
- Configure private VLANs for port isolation
- Set the speed/duplex mode for any port
- Configure the bandwidth of any port by rate limiting
- Configure up to 127 IEEE 802.1Q VLANs
- Enable GVRP automatic VLAN registration
- Upload and download of system firmware via TFTP
- Upload and download of switch configuration files via TFTP
- Configure Spanning Tree parameters
- Configure Class of Service (CoS) priority queuing
- Configure up to four static trunks
- Enable port mirroring
- DHCP filtering
- Set broadcast storm control on any port
- Display system information and statistics
- Configure port authentication

- RADIUS client support
- MAC filtering security

Required Connections

The switch provides an RS-232 serial port that enables a connection to a PC or terminal for monitoring and configuring the switch. A null-modem console cable is provided with the switch.

Attach a VT100-compatible terminal, or a PC running a terminal emulation program to the switch. You can use the console cable provided with this package, or use a null-modem cable that complies with the wiring assignments shown in Appendix B.

To connect a terminal to the console port, complete the following steps:

1. Connect the console cable to the serial port on a terminal, or a PC running terminal emulation software, and tighten the captive retaining screws on the DB-9 connector.
2. Connect the other end of the cable to the RS-232 serial port on the switch.
3. Make sure the terminal emulation software is set as follows:
 - Select the appropriate serial port (COM port 1, or COM port 2).
 - Set the data rate to 9600 baud.
 - Set the data format to 8 data bits, 1 stop bit, and no parity.
 - Set flow control to none.
 - Set the emulation mode to VT100.
 - When using HyperTerminal, select Terminal keys, not Windows keys.

Note: When using HyperTerminal with Microsoft® Windows® 2000, make sure that you have Windows 2000 Service Pack 2 or later installed. Windows 2000 Service Pack 2 fixes the problem of arrow keys not functioning in HyperTerminal's VT100 emulation. See www.microsoft.com for information on Windows 2000 service packs.

4. Once you have set up the terminal correctly, the console login screen will be displayed.

Note: Refer to “IGMP Snooping Commands” on page 3-61 for a complete description of console configuration options.

For a description of how to use the CLI, see “Using the Command Line Interface” on page 3-1. For a list of all the CLI commands and detailed information on using the CLI, refer to “Command Groups” on page 3-10.

Remote Connections

Prior to accessing the switch's onboard agent via a network connection, configure it with a valid IP address, subnet mask, and default gateway using a console connection, DHCP or BOOTP protocol.

The IP address for this switch is unassigned by default. To manually configure this address or enable dynamic address assignment via DHCP or BOOTP, see “Setting an IP Address” on page 1-7.

Note: This switch supports four concurrent Telnet sessions.

After configuring the switch's IP parameters, you can access the onboard configuration program from anywhere within the attached network. The onboard configuration program can be accessed using Telnet from any computer attached to the network. The switch can also be managed by any computer using a Web

browser (Internet Explorer 5.0 or above, or Netscape Navigator 6.2 or above), or from a network computer using network management software.

Note: The onboard program only provides access to basic configuration functions. To access the full range of SNMP management functions, you must use SNMP-based network management software.

Basic Configuration

Console Connection

The CLI program provides two different command levels — normal access level (Normal Exec) and privileged access level (Privileged Exec). The commands available at the Normal Exec level are a limited subset of those available at the Privileged Exec level and only allow you to display information and use basic utilities. To fully configure switch parameters, you must access the CLI at the Privileged Exec level.

Access to both CLI levels are controlled by user names and passwords. The switch has a default user name and password for each level. To log into the CLI at the Privileged Exec level using the default user name and password, perform these steps:

1. To initiate your console connection, press <Enter>. The “User Access Verification” procedure starts.
2. At the Username prompt, enter “admin.”
3. At the Password prompt, also enter “admin.” (The password characters are not displayed on the console screen.)
4. The session is opened and the CLI displays the “Console#” prompt indicating you have access at the Privileged Exec level.

Setting Passwords

Note: If this is your first time to log into the CLI program, you should define new passwords for both default user names using the “username” command, record them and put them in a safe place.

Passwords can consist of up to 8 alphanumeric characters and are case sensitive. To prevent unauthorized access to the switch, set the passwords as follows:

1. Open the console interface with the default user name and password “admin” to access the Privileged Exec level.
2. Type “configure” and press <Enter>.
3. Type “username guest password 0 *password*,” for the Normal Exec level, where *password* is your new password. Press <Enter>.
4. Type “username admin password 0 *password*,” for the Privileged Exec level, where *password* is your new password. Press <Enter>.

```
Username: admin
Password:
```

```
CLI session with the TigerSwitch 10/100 -
6724L2 Managed 24+2 Standalone Switch is opened.
To end the CLI session, enter [Exit].
```

```
Console#configure
Console(config)#username guest password 0 [password]
Console(config)#username admin password 0 [password]
Console(config)#
```

Setting an IP Address

You must establish IP address information for the switch to obtain management access through the network. This can be done in either of the following ways:

Manual — You have to input the information, including IP address and subnet mask. If your management station is not in the same IP subnet as the switch, you will also need to specify the default gateway router.

Dynamic — The switch sends IP configuration requests to BOOTP or DHCP address allocation servers on the network.

Note: Only one VLAN interface can be assigned an IP address (the default is VLAN 1). This defines the management VLAN, the only VLAN through which you can gain management access to the switch. If you assign an IP address to any other VLAN, the new IP address overrides the original IP address and this becomes the new management VLAN.

Manual Configuration

You can manually assign an IP address to the switch. You may also need to specify a default gateway that resides between this device and management stations that exist on another network segment. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. Anything outside this format will not be accepted by the CLI program.

Note: The IP address for this switch is unassigned by default.

Before you can assign an IP address to the switch, you must obtain the following information from your network administrator:

- IP address for the switch

- Default gateway for the network
- Network mask for this network

To assign an IP address to the switch, complete the following steps:

1. From the Privileged Exec level global configuration mode prompt, type “interface vlan 1” to access the interface-configuration mode. Press <Enter>.
2. Type “ip address *ip-address netmask*,” where “ip-address” is the switch IP address and “netmask” is the network mask for the network. Press <Enter>.
3. Type “exit” to return to the global configuration mode prompt. Press <Enter>.
4. To set the IP address of the default gateway for the network to which the switch belongs, type “ip default-gateway *gateway*,” where “gateway” is the IP address of the default gateway. Press <Enter>.

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.5 255.255.255.0
Console(config-if)#exit
Console(config)#ip default-gateway 192.168.1.254
Console(config)#
```

Dynamic Configuration

If you select the “bootp” or “dhcp” option, IP will be enabled but will not function until a BOOTP or DHCP reply has been received. You therefore need to use the “ip dhcp restart” command to start broadcasting service requests. Requests will be sent periodically in an effort to obtain IP configuration information. (BOOTP and DHCP values can include the IP address, subnet mask, and default gateway.)

If the “bootp” or “dhcp” option is saved to the startup-config file (step 6), then the switch will start broadcasting service requests as soon as it is powered on.

To automatically configure the switch by communicating with BOOTP or DHCP address allocation servers on the network, complete the following steps:

1. From the Global Configuration mode prompt, type “interface vlan 1” to access the interface-configuration mode. Press <Enter>.
2. At the interface-configuration mode prompt, use one of the following commands:
 - To obtain IP settings via DHCP, type “ip address dhcp” and press <Enter>.
 - To obtain IP settings via BOOTP, type “ip address bootp” and press <Enter>.
3. Type “end” to return to the Privileged Exec mode. Press <Enter>.
4. Type “ip dhcp restart” to begin broadcasting service requests. Press <Enter>.
5. Wait a few minutes, and then check the IP configuration settings by typing the “show ip interface” command. Press <Enter>.

6. Then save your configuration changes by typing “copy running-config startup-config.” Enter the startup file name and press <Enter>.

```
Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
Console(config-if)#exit
Console#ip dhcp restart
Console#show ip interface
IP interface vlan
  IP address and netmask: 10.1.0.54 255.255.255.0 on VLAN 1,
  and address mode: User specified.
Console#copy running-config startup-config
Startup configuration file name []: startup

Console#
```

Enabling SNMP Management Access

The switch can be configured to accept management commands from Simple Network Management Protocol (SNMP) applications. You can configure the switch to (1) respond to SNMP requests or (2) generate SNMP traps.

When SNMP management stations send requests to the switch (either to return information or to set a parameter), the switch provides the requested data or sets the specified parameter. The switch can also be configured to send information to SNMP managers (without being requested by the managers) through trap messages, which inform the manager that certain events have occurred.

Community Strings

Community strings are used to control management access to SNMP stations, as well as to authorize SNMP stations to receive trap messages from the switch.

You therefore need to assign community strings to specified users or user groups, and set the access level.

The default strings are:

- **public** - with read-only access. Authorized management stations are only able to retrieve MIB objects.
- **private** - with read-write access. Authorized management stations are able to both retrieve and modify MIB objects.

Note: If you do not intend to utilize SNMP, it is recommended that you delete both of the default community strings. If there are no community strings, then SNMP management access to the switch is disabled.

To prevent unauthorized access to the switch via SNMP, it is recommended that you change the default community strings.

To configure a community string, complete the following steps:

1. From the Privileged Exec level global configuration mode prompt, type “snmp-server community *string mode*,” where “string” is the community access string and “mode” is **rw** (read/write) or **ro** (read only). Press <Enter>.
2. To remove an existing string, simply type “no snmp-server community *string*,” where “string” is the community access string to remove. Press <Enter>.

```
Console(config)#snmp-server community abc rw
Console(config)#snmp-server community private
Console(config)#
```

Trap Receivers

You can also specify SNMP stations that are to receive traps from the switch.

To configure a trap receiver, complete the following steps:

1. From the Privileged Exec level global configuration mode prompt, type “snmp-server host *host-address* *community-string*,” where “host-address” is the IP address for the trap receiver and “community-string” is the string associated with that host. Press <Enter>.
2. In order to configure the switch to send SNMP notifications, you must enter at least one snmp-server enable traps command. Type “snmp-server enable traps *type*,” where “type” is either **authentication** or **link-up-down**. Press <Enter>.

```
Console(config)#snmp-server enable traps link-up-down
Console(config)#
```

Saving Configuration Settings

Configuration commands only modify the running configuration file and are not saved when the switch is rebooted. To save all your configuration changes in nonvolatile storage, you must copy the running configuration file to the start-up configuration file using the “copy” command.

To save the current configuration settings, enter the following command:

1. From the Privileged Exec mode prompt, type “copy running-config startup-config” and press <Enter>.

2. Enter the name of the start-up file. Press <Enter>.

```
Console#copy running-config startup-config
Startup configuration file name []: startup
\Write to FLASH Programming.

\Write to FLASH finish.
Success.

Console#
```

Managing System Files

The switch's flash memory supports three types of system files that can be managed by the CLI program, Web interface, or SNMP. The switch's file system allows files to be uploaded and downloaded, copied, deleted, and set as a start-up file.

The three types of files are:

- **Configuration** — This file stores system configuration information and is created when configuration settings are saved. Saved configuration files can be selected as a system start-up file or can be uploaded via TFTP to a server for backup. A file named "Factory_Default_Config.cfg" contains all the system default settings and cannot be deleted from the system. See "Saving or Restoring Configuration Settings" on page 2-22 for more information.
- **Operation Code** — System software that is executed after boot-up, also known as run-time code. This code runs the switch operation and provides the CLI and Web management interfaces. See "Managing Firmware" on page 2-20 for more information.
- **Diagnostic Code** — Software that is run during system boot-up, also known as POST (Power On Self-Test). This code

also provides a facility to upload firmware files to the system directly through the console port. See “Upgrading Firmware via the Serial Port” on page B-1.

Due to the size limit of the flash memory, the switch supports only one operation code file, and two diagnostic code files. However, you can have as many configuration files as available flash memory space allows.

In the system flash memory, one file of each type must be set as the start-up file. During a system boot, the diagnostic and operation code files set as the start-up file are run, and then the start-up configuration file is loaded. Configuration files can also be loaded while the system is running; however, this will automatically reboot the switch.

System Defaults

The switch’s system defaults are provided in the configuration file “Factory_Default_Config.cfg.” To reset the switch defaults, this file should be set as the startup configuration file (page 2-22).

The following table lists some of the basic system defaults.

| Function | Parameter | Default |
|----------------|------------------|-----------|
| IP Settings | Management VLAN | 1 |
| | IP Address | 0.0.0.0 |
| | Subnet Mask | 255.0.0.0 |
| | Default Gateway | 0.0.0.0 |
| | DHCP | Disabled |
| | BOOTP | Disabled |
| Web Management | HTTP Server | Enabled |
| | HTTP Port Number | 80 |

| Function | Parameter | Default |
|-------------------------|---|---|
| SNMP | Community Strings | “public” (read only) “private” (read/write) |
| | Traps | Authentication traps: enabled Link-up-down events: enabled |
| Security | Privileged Exec Level | Username “admin” Password “admin” |
| | Normal Exec Level | Username “guest” Password “guest” |
| | Enable Privileged Exec from Normal Exec Level | Password “super” |
| | RADIUS Authentication | Disabled |
| Console Port Connection | Baud Rate | 9600 |
| | Data bits | 8 |
| | Stop bits | 1 |
| | Parity | none |
| | Local Console Timeout | 0 (disabled) |

| Function | Parameter | Default |
|------------------------|----------------------------------|--|
| Port Status | Admin Status | Enabled |
| | Auto-negotiation | Enabled |
| | Flow Control | Disabled |
| | 10/100 Mbps Port Capability | 10 Mbps half duplex 10 Mbps full duplex 100 Mbps half duplex 100 Mbps full duplex Full-duplex flow control disabled |
| | 10/100/1000 Mbps Port Capability | 10 Mbps half duplex 10 Mbps full duplex 100 Mbps half duplex 100 Mbps full duplex 1000 Mbps full duplex Symmetric flow control disabled |
| Link Aggregation | Static Trunks | None |
| Spanning Tree Protocol | Status | Enabled (Defaults: All values based on IEEE 802.1D) |
| | Fast Forwarding | Disabled |
| Address Table | Aging Time | 300 seconds |

| Function | Parameter | Default |
|----------------------------|-------------------------------|--|
| Virtual LANs | Default VLAN | 1 |
| | PVID | 1 |
| | Acceptable Frame Type | All |
| | Ingress Filtering | Disabled |
| | Switchport Mode (Egress Mode) | Untagged frames |
| | Private VLAN | No Private VLAN |
| | GVRP (global) | Disabled |
| | GVRP (port interface) | Disabled |
| Class of Service | Ingress Port Priority | 0 |
| | Weighted Round Robin | Class 0: 1 Class 1: 3 Class 2: 12 Class 3: 48 |
| Broadcast Storm Protection | Status | Enabled (all ports) |
| | Broadcast Limit Rate | 6% of buffer space |

CHAPTER 2

CONFIGURING THE SWITCH

Using the Web Interface

This switch provides an embedded HTTP Web agent. Using a Web browser you can configure the switch and view statistics to monitor network activity. The Web agent can be accessed by any computer on the network using a standard Web browser (Internet Explorer 5.0 or above, or Netscape Navigator 6.2 or above).

Note: You can also use the Command Line Interface (CLI) to manage the switch over a serial connection to the console port or via Telnet. For more information on using the CLI, refer to “Using the Command Line Interface.”

Prior to accessing the switch from a Web browser, first perform the following tasks:

1. Configure the switch with a valid IP address, subnet mask, and default gateway using an out-of-band serial connection, BOOTP or DHCP protocol. (See “Setting the IP Address” on page 2-11.)
2. Set user names and passwords using an out-of-band serial connection. Access to the Web agent is controlled by the same user names and passwords as the onboard configuration program. (See “Configuring the Logon Password” on page 2-15.)
3. After you enter a user name and password, you will have access to the system configuration program.

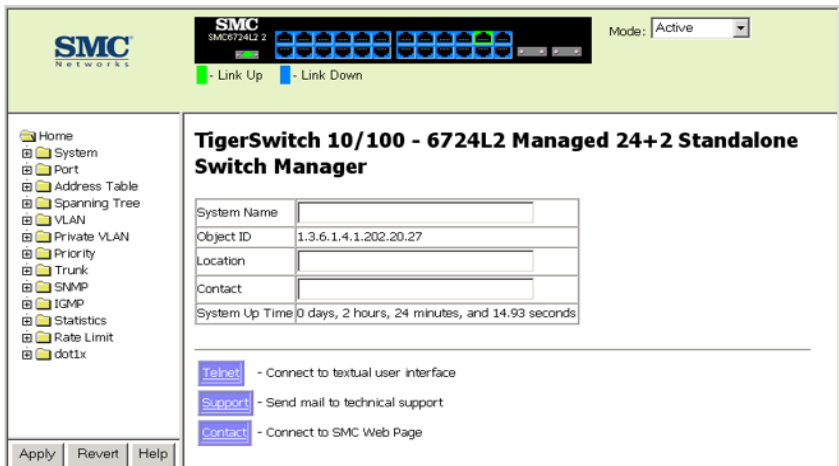
- Notes:**
- 1.** You are allowed three attempts to enter the correct password; on the third failed attempt the current connection is terminated.
 - 2.** If you log into the Web interface as guest (Normal Exec level), you can view page information but only change the guest password. If you log in as “admin” (Privileged Exec level), you can apply changes on all pages.
 - 3.** If the path between your management station and this switch does not pass through any device that uses the Spanning Tree Algorithm, you can set the switch port attached to your management station to fast forwarding to improve the switch’s response time to management commands issued through the Web interface. See “Managing STA Interface Settings” on page 2-47.

Navigating the Web Browser Interface

To access the Web-browser interface you must first enter a user name and password. The administrator has Read/Write access to all configuration parameters and statistics. The default user name and password for the administrator is “admin.”

Home Page

When your Web browser connects with the switch's Web agent, the home page is displayed as shown below. The home page displays the Main Menu on the left side of the screen and System Information on the right side. The Main Menu links are used to navigate to other menus, and display configuration parameters and statistics.



Configuration Options

Configurable parameters have a dialog box or a drop-down list. Once a configuration change has been made on a page, be sure to click on the “Apply” or “Apply Changes” button to confirm the

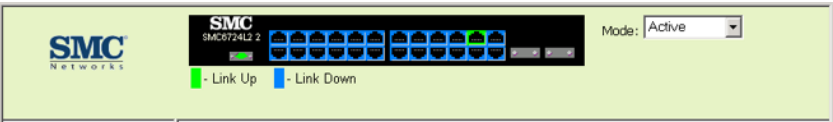
new setting. The following table summarizes the Web page configuration buttons.

| Button | Action |
|---------------|--|
| Revert | Cancels specified values and restores current values prior to pressing “Apply” or “Apply Changes.” |
| Refresh | Immediately updates values for the current page. |
| Apply | Sets specified values to the system. |
| Apply Changes | Sets specified values to the system. |

- Notes:**
- 1. To ensure proper screen refresh, be sure that Internet Explorer 5.x is configured as follows: Under the menu “Tools / Internet Options / General / Temporary Internet Files / Settings,” the setting for item “Check for newer versions of stored pages” should be “Every visit to the page.”
 - 2. When using Internet Explorer 5.0, you may have to manually refresh the screen after making configuration changes by pressing the browser’s refresh button.

Panel Display

The Web agent displays an image of the switch’s ports, indicating whether each link is up or down. Clicking on the image of a port opens the Port Configuration page as described on page 2-32.



Main Menu

Using the onboard Web agent, you can define system parameters, manage and control the switch, and all its ports, or monitor network conditions. The following table briefly describes the selections available from this program.

| Menu | Description | Page |
|------------------------|--|------|
| <i>System</i> | | |
| System Information | Provides basic system description, including contact information | 2-9 |
| IP | Sets the IP address for management access | 2-11 |
| Passwords | Assigns a new password for the logon user name | 2-15 |
| Radius | Configures RADIUS authentication parameters | 2-17 |
| Firmware | Manages code image files | 2-20 |
| Configuration | Manages switch configuration files | 2-22 |
| Reset | Restarts the switch | 2-24 |
| Bridge Extension | Shows the bridge extension parameters; enables GVRP VLAN registration protocol | 2-24 |
| Switch Information | Shows the number of ports, hardware/firmware version numbers, and power status | 2-28 |
| <i>Port</i> | | |
| Port Information | Displays port connection status | 2-30 |
| Trunk Information | Displays trunk connection status | 2-30 |
| Port Configuration | Configures port connection settings | 2-32 |
| Trunk Configuration | Configures trunk connection settings | 2-32 |
| Port Broadcast Control | Sets the broadcast storm threshold for each port | 2-34 |

| Menu | Description | Page |
|-------------------------|---|------|
| Trunk Broadcast Control | Sets the broadcast storm threshold for each trunk | 2-34 |
| Mirror | Sets the source and target ports for mirroring | 2-37 |
| <i>Address Table</i> | | |
| Static Addresses | Displays entries for interface or address | 2-39 |
| Dynamic Addresses | Displays or edits static entries in the Address Table | 2-40 |
| Address Aging | Sets timeout for dynamically learned entries | 2-42 |
| <i>Spanning Tree</i> | | |
| STA Information | Displays STA values used for the bridge | 2-45 |
| STA Configuration | Configures global bridge settings for STA | 2-47 |
| STA Port Information | Displays individual port settings for STA | 2-51 |
| STA Trunk Information | Displays individual trunk settings for STA | 2-51 |
| STA Port Configuration | Configures individual port settings for STA | 2-52 |
| STA Trunk Configuration | Configures individual trunk settings for STA | 2-52 |
| <i>VLAN</i> | | |
| VLAN Base Information | Displays information on VLAN types supported by this switch | 2-56 |
| VLAN Current Table | Shows the current port members of each VLAN and whether or not the port supports VLAN tagging | 2-57 |
| VLAN Static List | Used to create or remove VLAN groups | 2-59 |
| VLAN Static Table | Modifies the settings for an existing VLAN | 2-61 |
| VLAN Static Membership | Configures membership type for interfaces, including tagged, untagged or forbidden | 2-64 |
| VLAN Port Configuration | Specifies default PVID and VLAN attributes | 2-65 |

| Menu | Description | Page |
|----------------------------------|---|------|
| VLAN Trunk Configuration | Specifies default trunk VID and VLAN attributes | 2-65 |
| <i>Private VLAN</i> | | |
| Private VLAN Information | Shows private VLANs and associated ports | 2-69 |
| Private VLAN Configuration | Configures private VLANs | 2-71 |
| Private VLAN Association | Maps a secondary VLAN to a primary VLAN | 2-72 |
| Private VLAN Port Information | Shows VLAN port type, and associated primary or secondary VLANs | 2-73 |
| Private VLAN Port Configuration | Configures VLAN port type, and associated primary or secondary VLANs | 2-75 |
| Private VLAN Trunk Information | Shows VLAN trunk type, and associated primary or secondary VLANs | 2-73 |
| Private VLAN Trunk Configuration | Configures VLAN trunk type, and associated primary or secondary VLANs | 2-75 |
| Priority - Queue Mode | Sets the queue mode to strict service or Weighted Round-Robin | 2-78 |
| Trunk - Trunk Configuration | Specifies ports to group into static trunks | 2-79 |
| SNMP - SNMP Configuration | Configures community strings and related trap functions | 2-82 |

| Menu | Description | Page |
|--|---|-------|
| <i>IGMP</i> | | |
| IGMP Configuration | Enables multicast filtering; configures parameters for multicast query | 2-87 |
| Multicast Router Port Information | Displays the ports that are attached to a neighboring multicast router/switch for each VLAN ID | 2-89 |
| Static Multicast Router Port Configuration | Assigns ports that are attached to a neighboring multicast router/switch | 2-91 |
| IP Multicast Registration Table | Displays all multicast groups active on this switch, including multicast IP addresses and VLAN ID | 2-92 |
| IGMP Member Port Table | Indicates multicast addresses associated with the selected VLAN | 2-94 |
| Statistics - Port Statistics | Lists Ethernet and RMON port statistics | 2-96 |
| <i>Rate Limit</i> | | |
| Input Rate Limit Port Configuration | Sets the rate limit on input traffic for specified port | 2-98 |
| Input Rate Limit Trunk Configuration | Sets the rate limit on input traffic for specified trunk | 2-98 |
| Output Rate Limit Port Configuration | Sets the rate limit on output traffic for specified port | 2-98 |
| Output Rate Limit Trunk Configuration | Sets the rate limit on output traffic for specified trunk | 2-98 |
| <i>Port Authentication</i> | | |
| Information | Displays general port authentication status information | 2-100 |
| Configuration | Enables the changing of general port authentication features | 2-103 |

| Menu | Description | Page |
|--------------------|--|-------|
| Port Configuration | Enables the changing of port authentication features | 2-103 |
| Statistics | Displays a per-port statistical readout | 2-107 |

Basic Configuration

Displaying System Information

You can easily identify the system by providing a descriptive name, location and contact information.

Command Attributes

- **System Name** – Name assigned to the switch system.
- **Object ID** – MIB II object ID for switch's network management subsystem.
- **Location** – Specifies the system location.
- **Contact** – Administrator responsible for the system.
- **System Up Time** – Length of time the management agent has been up.
- **MAC Address**¹ – The physical layer address for this switch.
- **Web server**² – Shows if management access via HTTP is enabled or disabled.
- **Web server port**² – Shows the TCP port number used by the Web interface.
- **POST result**² – Shows results of the power-on self-test

1: Web: See "Setting the IP Address" on page 2-11.

2: CLI Only

Web – Click System, System Information. Specify the system name, location, and contact information for the system administrator, then click Apply. (This page also includes a Telnet button that allows access to the Command Line Interface via Telnet.)

Switch Information

Main Board:

| | |
|-----------------------|--------|
| Serial Number | 12345 |
| Number of Ports | 26 |
| Hardware Version | 012 |
| Internal Power Status | Active |

Management Software:

| | |
|------------------------|---------|
| Loader Version | 1.0.0.5 |
| Boot-ROM Version | 1.0.0.5 |
| Operation Code Version | 1.0.3.0 |
| Role | Master |

Expansion Slot:

| | |
|------------------|-------------|
| Expansion Slot 1 | not present |
| Expansion Slot 2 | not present |

CLI – Specify the hostname, location and contact information.

```

Console(config)#hostname R&D 5                               3-27
Console(config)#snmp-server location WC 9                     3-56
Console(config)#snmp-server contact Geoff                     3-55
Console#show system                                           3-36
System description: TigerSwitch 10/100 - 6724L2 Managed 24+2
                    Standalone Switch
System OID string: 1.3.6.1.4.1.259.6.10.42
System information
  System Up time: 0 days, 1 hours, 1 minutes, and 41.64 seconds
  System Name      : R&D 5
  System Location   : WC 9
  System Contact    : Geoff
  MAC address       : 00-55-FF-FF-DD-DD
  Web server        : enable
  Web server port   : 80
  POST result
  --- Performing Power-On Self Tests (POST) ---
  UART Loopback Test.....PASS
  Flash Memory Checksum Test.....PASS
  CPU Self Test.....PASS
  MPC850 clock Timer and Interrupt TEST...PASS
  WatchDog Timer and Interrupt Test.....PASS
  DRAM Test.....PASS
  ACD Chip Test.....PASS
  Switch Driver Initialization.....PASS
  Switch Internal Loopback Test .....PASS
  ----- DONE -----
Console#

```

Setting the IP Address

The IP address for this switch is unassigned by default. To manually configure an address, you need to change the switch's default settings (IP address 0.0.0.0 and netmask 255.0.0.0) to values that are compatible with your network. You may also need to establish a default gateway between the switch and management stations that exist on another network segment.

You can manually configure a specific IP address, or direct the device to obtain an address from a BOOTP or DHCP server. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. Anything outside this format will not be accepted by the configuration program.

Command Attributes

- **Management VLAN** – This is the only VLAN through which you can manage the switch. By default, all ports on the switch are members of VLAN 1, so a management station can be connected to any port on the switch. However, if you change the Management VLAN to another VLAN, you will lose access to the switch unless the management port has already been configured as a member of the new VLAN. If you lose access, you can reconnect the management station to a port that is a member of the Management VLAN or use the console interface to add the management port to the newly configured Management VLAN. (See “switchport allowed vlan” on page 129.)
- **IP Address Mode** – Specifies whether IP functionality is enabled via manual configuration (Static), Dynamic Host Configuration Protocol (DHCP), or Boot Protocol (BOOTP). If DHCP/BOOTP is enabled, IP will not function until a reply has been received from the server. Requests will be broadcast periodically by the switch for IP configuration settings. (DHCP/BOOTP values can include the IP address, subnet mask, and default gateway.)
- **IP Address** – Address of the VLAN interface that is allowed management access. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. (Default: 0.0.0.0)
- **Subnet Mask** – This mask identifies the host address bits used for routing to specific subnets. (Default: 255.0.0.0)
- **Gateway IP Address** – IP address of the gateway router between this device and management stations that exist on other network segments. (Default: 0.0.0.0)
- **MAC Address** – The physical layer address for this switch.

Manual Configuration

Web – Click System, IP. Specify the management interface, IP address and default gateway, then click Apply.

| IP Configuration | |
|--------------------|-------------------|
| Management VLAN | 1 |
| IP Address Mode | Static |
| IP Address | 10.1.0.3 |
| Subnet Mask | 255.255.255.0 |
| Gateway IP Address | 10.1.0.254 |
| MAC Address | 00-55-FF-FF-DD-DD |
| Restart DHCP | |

CLI – Specify the management interface, IP address and default gateway.

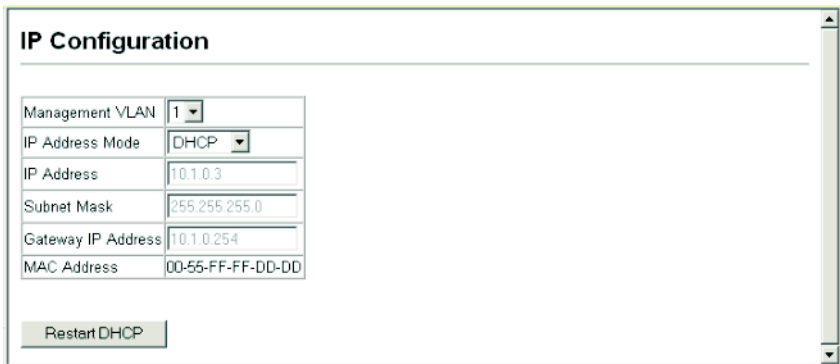
```

Console#config
Console(config)#interface vlan 1
Console(config-if)#ip address 10.1.0.3 255.255.255.0
Console(config-if)#exit
Console(config)#ip default-gateway 10.1.0.254
Console(config)#
  
```

Using DHCP/BOOTP

If your network provides DHCP/BOOTP services, you can configure the switch to be dynamically configured by these services.

Web – Click System, IP. Specify the Management VLAN, and set the IP Address Mode to DHCP or BOOTP. Click Apply to save your changes. Then click Restart DHCP to immediately request a new address. Note that the switch will also broadcast a request for IP configuration settings on the each power reset.



The screenshot shows a web interface titled "IP Configuration". It contains a form with the following fields and values:

| | |
|--------------------|-------------------|
| Management VLAN | 1 |
| IP Address Mode | DHCP |
| IP Address | 10.1.0.3 |
| Subnet Mask | 255.255.255.0 |
| Gateway IP Address | 10.1.0.254 |
| MAC Address | 00-55-FF-FF-DD-DD |

Below the form is a button labeled "Restart DHCP".

Note: If you lose your management connection, use a console connection and enter “show ip interface” to determine the new switch address.

CLI – Specify the management interface, set the IP Address Mode to DHCP or BOOTP, and then enter the “ip dhcp restart” command.

```
Console#config
Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
Console(config-if)#end
Console#ip dhcp restart
Console#show ip interface
IP address and netmask: 10.1.0.3 255.255.255.0 on VLAN 1,
and address mode: Dhcp.
Console#
```

Renewing DHCP – DHCP may lease addresses to clients indefinitely or for a specific period of time. If the address expires or the switch is moved to another network segment, you will lose management access to the switch. In this case, you can reboot the switch or submit a client request to restart DHCP service.

Web – If the address assigned by DHCP is no longer functioning, you will not be able to renew the IP settings via the Web interface. You can only restart DHCP service via the Web interface if the current address is still available.

CLI – Enter the following command to restart DHCP service.

```
Console#ip dhcp restart
```

3-81

Configuring User Authentication

Use the Passwords or Radius menu to restrict management access based on specified user names and passwords. You can manually configure access rights on the switch (Passwords menu), or you can use a remote access authentication server based on the RADIUS protocol (Radius menu).

Configuring the Logon Password

The guest only has read access for most configuration parameters. However, the administrator has write access for all parameters governing the onboard agent. You should therefore assign a new administrator password as soon as possible, and store it in a safe place. (If for some reason your password is lost, you can reload the factory default settings to restore the default password as described in “Upgrading Firmware via the Serial Port” on page B-1.)

The default guest name is “guest” with the password “guest.” The default administrator name is “admin” with the password “admin.” Note that user names can only be assigned via the CLI.

Command Attributes

- **User Name*** – The name of the user.
(Maximum length: 8 characters; maximum number of users: 16)
- **Access Level*** – Specifies the user level.
(Options: Normal and Privileged.)
- **Password** – Specifies the user password.
(Maximum length: 8 characters plain text, case sensitive)

* CLI only.

Web – Click System, Passwords. To change the password for the current user, enter the old password, enter the new password, confirm it by entering it again, then click Apply.

| Passwords | |
|------------------|--------------------------|
| Old Password | <input type="password"/> |
| New Password | <input type="password"/> |
| Confirm Password | <input type="password"/> |

CLI – Assign a user name and access-level 15 (i.e., administrator), then specify the password.

```
Console(config)#username bob access-level 15
Console(config)#username bob password 0 smith
Console(config)#
```

3-27

Configuring RADIUS Logon Authentication

Remote Authentication Dial-in User Service (RADIUS) is a logon authentication protocol that uses software running on a central server to control access to RADIUS-compliant devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user or group that require management access to a switch.

Command Usage

- By default, management access is always checked against the authentication database stored on the local switch. If a remote authentication server is used, you must specify the authentication sequence and the corresponding parameters for the remote authentication protocol.
- RADIUS uses UDP, which only offers best-effort delivery. Also, RADIUS encrypts only the password in the access-request packet from the client to the server.
- RADIUS logon authentication assigns a specific privilege level for each user name/password pair. The user name, password, and privilege level must be configured on the authentication server.
- You can specify one to two authentication methods for any user to indicate the authentication sequence. For example, if you select (1) RADIUS and (2) Local, the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then the local user name and password is checked.

Command Attributes

- **Authentication** – Select the authentication, or authentication sequence required:
 - **Radius** – User authentication is performed using a RADIUS server only.
 - **Local** – User authentication is performed only locally by the switch.
 - **Radius, Local** – User authentication is attempted first using a RADIUS server, then locally by the switch.
 - **Local, Radius** – User authentication is first attempted locally by the switch, then using a RADIUS server.
- **Server IP Address** – Address of authentication server.
(Default: 10.1.0.1)
- **Server Port Number** – Network (UDP) port of authentication server used for authentication messages. (Range: 1-65535; Default: 1812)
- **Secret Text String** – Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 20 characters)
- **Number of Server Transmits** – Number of times the switch will try to authenticate logon access via the authentication server. (Range: 1-30; Default: 2)
- **Timeout for a reply** – The number of seconds the switch waits for a reply from the RADIUS server before it resends the request. (Range: 1-65535; Default: 5)

Note: The local switch user database has to be set up by manually entering user names and passwords using the CLI.

Web – Click System, Radius. To configure local or remote authentication preferences, specify the authentication sequence (i.e., one to two methods), fill in the parameters for RADIUS authentication if selected, and click Apply.

| Radius Settings | |
|----------------------------|----------|
| Authentication | Local |
| Server IP Address | 10.1.0.1 |
| Server Port Number | 1812 |
| Secret Text String | |
| Number of Server Transmits | 2 |
| Timeout for a reply (sec) | 5 |

CLI – Specify all the required parameters to enable logon authentication.

| | |
|---|------|
| Console(config)#authentication login radius | 3-39 |
| Console(config)#radius-server host 192.168.1.25 | 3-40 |
| Console(config)#radius-server port 181 | 3-41 |
| Console(config)#radius-server key green | 3-42 |
| Console(config)#radius-server retransmit 5 | 3-42 |
| Console(config)#radius-server timeout 10 | 3-43 |
| Console#show radius-server | 3-43 |
| Server IP address: 192.168.1.25 | |
| Communication key with radius server: | |
| Server port number: 181 | |
| Retransmit times: 5 | |
| Request timeout: 10 | |
| Console(config)# | |

Managing Firmware

You can upload/download firmware to or from a TFTP server. By saving runtime code to a file on a TFTP server, that file can later be downloaded to the switch to restore operation.

Command Attributes

- **TFTP Server IP Address** – The IP address of a TFTP server.
- **Destination File Name** – The file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the TFTP server is 127 characters or 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, “.”, “-”, “_”)

Note: Only one copy of the system software (i.e., the runtime firmware) can be stored in the file directory on the switch. The system software file cannot be deleted.

Downloading System Software from a Server

When downloading runtime code, you must select “Destination File Name” to replace the current image. This switch can only contain one operation code file.

Web – Click System, Firmware. Enter the IP address of the TFTP server, enter the file name of the software to download, enter the Destination File Name to overwrite the current file on the switch then click **Transfer from Server**. To start the new firmware, reboot the system via the Reset menu.

Transfer Operation Code Image File from Server

| | |
|--------------------------------|-----------------|
| Current Operation Code Version | 2.0.0.31 |
| TFTP Server IP Address | 0.0.0.0 |
| Source File Name | |
| Destination File Name | runtime2.0.0.31 |

CLI – Enter the IP address of the TFTP server, select “config” or “opcode” file type, then enter the source and destination file names, set the new file to start up the system, and then restart the switch.

| | |
|---|------|
| Console#copy tftp file | 3-20 |
| TFTP server ip address: 10.1.0.19 | |
| Choose file type: | |
| 1. config: 2. opcode: <1-2>: 2 | |
| Source file name: ACD_v1.0.0.8.bix | |
| Destination file name: acd | |
| \Write to FLASH Programming. | |
| -Write to FLASH finish. | |
| Success. | |
| Console#config | |
| Console(config)#boot system opcode: acd | 3-25 |
| Console(config)#exit | |
| Console#reload | 3-17 |

Saving or Restoring Configuration Settings

You can upload/download configuration settings to/from a TFTP server. The configuration file can be later downloaded to restore the switch's settings.

Command Attributes

- **TFTP Server IP Address** – The IP address of a TFTP server.
- **Destination File Name** — The configuration file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the TFTP server is 127 characters or 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")

Note: The maximum number of user-defined configuration files is limited only by available Flash memory space.

Downloading Configuration Settings from a Server

You can download the configuration file under a new file name and then set it as the startup file, or you can specify the current startup configuration file as the destination file to directly replace it. Note that the file "Factory_Default_Config.cfg" can be copied to the TFTP server, but cannot be used as the destination on the switch.

Web – Click System, Configuration. Enter the IP address of the TFTP server, enter the name of the file to download, select a file on the switch to overwrite or specify a new file name, and then click **Transfer from Server**.

Transfer Configuration File from Server

TFTP Server IP Address: 10.1.0.19

Source File Name: config-1

Destination File Name: ☐ (none) ☒ startup

Transfer from Server

If you download to a new file name, select the new file from the drop-down box for Startup Configuration File, and press Apply Changes. To use the new settings, reboot the system with the System/Reset command or reset power to the switch.

Start-Up Configuration File

File Name: startup

Apply Changes

CLI – Enter the IP address of the TFTP server, specify the source file on the server, set the startup file name on the switch, and then restart the switch.

```

Console#copy tftp startup-config
TFTP server ip address: 10.1.0.19
Source configuration file name: config-1
Startup configuration file name [] : startup
\Write to FLASH Programming.
-Write to FLASH finish.
Success.

Console#reload
Console#

```

3-20

If you download the startup configuration file under a new file name, you can set this file as the startup file at a later time, and then restart the switch.

| | |
|---|------|
| Console#config | |
| Console(config)#boot system config: startup-new | 3-25 |
| Console(config)#exit | |
| Console#reload | 3-17 |

Resetting the System

Web – Click System, Reset. Click the Reset button to restart the switch.

Reset the switch by selecting 'Reset'.

Reset

CLI – Use the reload command to restart the switch.

| | |
|---|------|
| Console#reload | 3-17 |
| System will be restarted, continue <y/n>? | |

Note: When restarting the system, it will always run the Power-On Self-Test.

Displaying Bridge Extension Capabilities

The Bridge MIB includes extensions for managed devices that support Multicast Filtering, Traffic Classes, and Virtual LANs. You can access these extensions to display default settings for the key variables, or to configure the global setting for GARP VLAN Registration Protocol (GVRP).

Command Attributes

- **Extended Multicast Filtering Services** – This switch does not support the filtering of individual multicast addresses based on GMRP (GARP Multicast Registration Protocol).
- **Traffic Classes** – This switch provides mapping of user priorities to multiple traffic classes. (Refer to “Class of Service Configuration” on page 2-77.)
- **Static Entry Individual Port** – This switch allows static filtering for unicast and multicast addresses. (Refer to “Setting Static Addresses” on page 2-39.)
- **VLAN Learning** – This switch uses Shared VLAN Learning (SVL), where each port shares a common filtering database.
- **Configurable PVID Tagging** – This switch allows you to override the default Port VLAN ID (PVID used in frame tags) and egress status (VLAN-Tagged or Untagged) on each port. (Refer to “VLAN Configuration” on page 2-52.)
- **Local VLAN Capable** – This switch does not support multiple local bridges; i.e., multiple Spanning Trees.
- **GMRP** – GARP Multicast Registration Protocol (GMRP) allows network devices to register endstations with multicast groups. This switch does not support GMRP; it uses the Internet Group Management Protocol (IGMP) to provide automatic multicast filtering.
- **GVRP** – GARP VLAN Registration Protocol (GVRP) defines a way for switches to exchange VLAN information in order to register necessary VLAN members on ports across the network. This function should be enabled to permit VLANs groups which extend beyond the local switch. (Default: Enabled)

Web – Click System, Bridge Extension.

Bridge Capability

| | |
|---------------------------------------|---------|
| Extended Multicast Filtering Services | No |
| Traffic Classes | Enabled |
| Static Entry Individual Port | Yes |
| VLAN Learning | SVL |
| Configurable PVID Tagging | Yes |
| Local VLAN Capable | No |

| | |
|-----------------|--|
| Traffic Classes | <input checked="" type="checkbox"/> Enable |
| GMRP | <input type="checkbox"/> Enable |
| GVRP | <input checked="" type="checkbox"/> Enable |

CLI – Enter the following command.

```
Console#show bridge-ext
Max support vlan numbers: 127
Max support vlan ID: 4094
Extended multicast filtering services: No
Static entry individual port: Yes
VLAN learning: SVL
Configurable PVID tagging: Yes
Local VLAN capable: No
Traffic classes: Enabled
Global GVRP status: Enabled
GMRP: Disabled
Console#
```

3-145

Enabling or Disabling GVRP (Global Setting)

GARP VLAN Registration Protocol (GVRP) defines a way for switches to exchange VLAN information in order to register VLAN members on ports across the network. VLANs are dynamically configured based on join messages issued by host devices and propagated throughout the network. GVRP must be enabled to permit automatic VLAN registration, and to support VLANs which extend beyond the local switch. (Default: Enabled)

Web – Click System, Bridge Extension. Enable or disable GVRP, click Apply

| Bridge Capability | |
|---------------------------------------|---------|
| Extended Multicast Filtering Services | No |
| Traffic Classes | Enabled |
| Static Entry Individual Port | Yes |
| VLAN Learning | SVL |
| Configurable PVID Tagging | Yes |
| Local VLAN Capable | No |

| | |
|-----------------|--|
| Traffic Classes | <input checked="" type="checkbox"/> Enable |
| GMRP | <input type="checkbox"/> Enable |
| GVRP | <input checked="" type="checkbox"/> Enable |

CLI – This example enables GVRP for the switch.

```
Console(config)#bridge-ext gvrp  
Console(config)#
```

3-144

Displaying Switch Hardware/Software Versions

Use the Switch Information page to display hardware/firmware version numbers for the main board and management software, as well as the power status of the system.

Command Attributes

Main Board

- **Serial Number** – The serial number of the switch.
- **Number of Ports** – Number of built-in RJ-45 ports and expansion ports.
- **Hardware Version** – Hardware version of the main board.
- **Internal Power Status** – Displays the status of the internal power supply.

Management Software

- **Loader Version** – Version number of loader code.
- **Boot-ROM Version** – Version number of Power-On Self-Test (POST) and boot code.
- **Operation Code Version** – Version number of runtime code.
- **Role** – Shows that this switch is operating as Master (i.e., operating stand-alone).

Expansion Slots

- **Expansion Slot** – Indicates any installed module type.

Web – Click System, Switch Information.

Switch Information

Main Board:

| | |
|-----------------------|--------|
| Serial Number | 12345 |
| Number of Ports | 26 |
| Hardware Version | 012 |
| Internal Power Status | Active |

Management Software:

| | |
|------------------------|---------|
| Loader Version | 1.0.0.5 |
| Boot-ROM Version | 1.0.0.5 |
| Operation Code Version | 1.0.3.0 |
| Role | Master |

Expansion Slot:

| | |
|------------------|-------------|
| Expansion Slot 1 | not present |
| Expansion Slot 2 | not present |

CLI – Use the following command to display version information.

```

Console#show version
Unit1
  Serial number      :12345
  Hardware version   :012
  Module A type      :not present
  Module B type      :not present
  Number of ports    :26
  Main power status  :up
Agent(master)
  Unit id            :1
  Loader version     :1.0.0.5
  Boot rom version   :1.0.0.5
  Operation code version :1.0.1.1
Console#
  
```

3-37

Port Configuration

Displaying Connection Status

You can use the Port Information or Trunk Information pages to display the current connection status, including link state, speed/duplex mode, flow control, and auto-negotiation.

Command Attributes

- **Name** – Interface label.
- **Type** – Indicates the port type (100BASE-TX, 1000BASE-T, 1000BASE-SX, 1000BASE-LX or 100BASE-FX).
- **Admin Status** – Shows if the interface is enabled or disabled.
 - Web - Displays Enabled or Disabled.
 - CLI - Displays Port Admin (up or down).
- **Link Status** – Indicates if the link is Up or Down. (CLI only)
- **Oper Status** – Indicates if the link is Up or Down. (Web only)
- **Port Operation Status** – Provides detailed information on port state.
 - CLI only; displays this item only if the link is up.
- **Speed/Duplex Status** – Shows the current speed and duplex mode.
- **Flow Control Status** – Indicates the type of flow control currently in use.
 - Web - IEEE 802.3x, Back-Pressure or None.
 - CLI - Enabled or Disabled. Flow Type shows IEEE 802.3x, Back-Pressure or None.
- **Autonegotiation** – Shows if auto-negotiation is enabled or disabled.

- **MAC Address** – The physical layer address for this port.
 - CLI only; to access this on the Web, see “Setting the IP Address” on page -11.
- **Trunk Member** – Shows if port is a trunk member. (Port Information only)
- **Creation** – Shows if a trunk is manually configured. (Trunk Information only)
- **Port Capabilities*** – Specifies the capabilities to be advertised for a port during auto-negotiation. The following capabilities are supported:
 - **10half** - Supports 10 Mbps half-duplex operation
 - **10full** - Supports 10 Mbps full-duplex operation
 - **100half** - Supports 100 Mbps half-duplex operation
 - **100full** - Supports 100 Mbps full-duplex operation
 - **1000full** - Supports 1000 Mbps full-duplex operation
 - **Sym** - Transmits and receives pause frames for flow control
 - **FC** - Supports flow control

*To access this item on the Web, see “Configuring Interface Connections” on page -32.

Web – Click Port, Port Information or Trunk Information.

| Port Information | | | | | | | | |
|------------------|------|------------|--------------|-------------|---------------------|---------------------|-----------------|--------------|
| Port | Name | Type | Admin Status | Oper Status | Speed Duplex Status | Flow Control Status | Autonegotiation | Trunk Member |
| 1 | | 100Base-TX | Enabled | Up | 100full | IEEE 802.3x | Disabled | |
| 2 | | 100Base-TX | Enabled | Down | 10half | None | Enabled | |
| 3 | | 100Base-TX | Enabled | Down | 10half | None | Enabled | |
| 4 | | 100Base-TX | Enabled | Down | 10half | None | Enabled | |
| 5 | | 100Base-TX | Enabled | Down | 10half | None | Enabled | |

CLI – This example shows the connection status for Port 13.

```
Console#show interfaces status ethernet 1/13 3-99
Information of Eth 1/13
Basic information:
  Port type: 100TX
  Mac address: 00-55-FF-FF-DD-EA
Configuration:
  Name:
  Port admin: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full,
  Broadcast storm: Enabled
  Broadcast storm limit: 6 percent
  Flow control: Disabled
Current status:
Link status: Up
  Port operation status: Up
  Operation speed-duplex: 100full
  Flow control type: None
Console#
```

Configuring Interface Connections

You can use the Port Configuration or Trunk Configuration page to enable/disable an interface, set auto-negotiation and the interface capabilities to advertise, or manually fix the speed, duplex mode, and flow control. All switches have to comply with the Cisco EtherChannel standard.

Command Attributes

- **Name** – Allows you to label an interface. (Range: 1-64 characters)
- **Admin** – Allows you to manually disable an interface. You can disable an interface due to abnormal behavior (e.g., excessive collisions), and then reenable it after the problem has been resolved. You may also disable an interface for security reasons.
- **Speed/Duplex*** – Allows you to manually set the port speed and duplex mode.

- **Flow Control*** – Allows you to manually enable or disable flow control.
- **Autonegotiation (Port Capabilities)** – Allows auto-negotiation to be enabled/disabled. When auto-negotiation is enabled, you need to specify the capabilities to be advertised. When auto-negotiation is disabled, you can force the settings for speed, mode, and flow control. The following capabilities are supported.
 - **10half** - Supports 10 Mbps half-duplex operation
 - **10full** - Supports 10 Mbps full-duplex operation
 - **100half** - Supports 100 Mbps half-duplex operation
 - **100full** - Supports 100 Mbps full-duplex operation
 - **1000full** - Supports 1000 Mbps full-duplex operation
 - **Sym** (Gigabit only) - Check this item to transmit and receive pause frames, or clear it to auto-negotiate the sender and receiver for asymmetric pause frames. (*The current switch chip only supports symmetric pause frames.*)
 - **FC** - Supports flow control
 - Flow control can eliminate frame loss by “blocking” traffic from end stations or segments connected directly to the switch when its buffers fill. When enabled, back pressure is used for half-duplex operation and IEEE 802.3x for full-duplex operation. (Avoid using flow control on a port connected to a hub unless it is actually required to solve a problem. Otherwise back pressure jamming signals may degrade overall performance for the segment attached to the hub.)
- **Trunk** – Indicates if a port is a member of a trunk. To create trunks and select port members, see “Port Trunk Configuration” on page 2-79.

*Auto-negotiation must be disabled before you can configure or force the interface to use the Speed/Duplex Mode or Flow Control options.

Web – Click Port, Port Configuration or Trunk Configuration. Modify the required interface settings, and click Apply.

| Port Configuration | | | | | | | | |
|--------------------|----------|--|--------------|--------------|-----------------|---|--|-------|
| Port | Name | Admin | Speed Duplex | Flow Control | Autonegotiation | | | Trunk |
| 1 | | <input checked="" type="checkbox"/> Enable | 100full | Disabled | Enabled | <input checked="" type="checkbox"/> 10h <input checked="" type="checkbox"/> 100h <input type="checkbox"/> 1000h <input type="checkbox"/> Sym <input checked="" type="checkbox"/> 10f <input checked="" type="checkbox"/> 100f <input type="checkbox"/> 1000f <input type="checkbox"/> FC | | |
| 2 | | <input checked="" type="checkbox"/> Enable | 100full | Disabled | Enabled | <input checked="" type="checkbox"/> 10h <input checked="" type="checkbox"/> 100h <input type="checkbox"/> 1000h <input type="checkbox"/> Sym <input checked="" type="checkbox"/> 10f <input checked="" type="checkbox"/> 100f <input type="checkbox"/> 1000f <input type="checkbox"/> FC | | |
| 3 | RD SW#13 | <input checked="" type="checkbox"/> Enable | 100half | Enabled | Enabled | <input type="checkbox"/> 10h <input checked="" type="checkbox"/> 100h <input type="checkbox"/> 1000h <input type="checkbox"/> Sym <input type="checkbox"/> 10f <input checked="" type="checkbox"/> 100f <input type="checkbox"/> 1000f <input checked="" type="checkbox"/> FC | | |

CLI – Select the interface, and then enter the required settings.

```

Console(config)#interface ethernet 1/3                               3-89
Console(config-if)#description RD SW#13                             3-90
Console(config-if)#shutdown                                          3-98
.
Console(config-if)#no shutdown
Console(config-if)#no negotiation                                   3-92
Console(config-if)#speed-duplex 100half                             3-90
Console(config-if)#flowcontrol                                       3-94
.
Console(config-if)#negotiation
Console(config-if)#capabilities 100half                             3-93
Console(config-if)#capabilities 100full
Console(config-if)#capabilities flowcontrol
Console(config-if)#

```

Setting Broadcast Storm Thresholds

Broadcast storms may occur when a device on your network is malfunctioning, or if application programs are not well designed or properly configured. If there is too much broadcast traffic on your network, performance can be severely degraded or everything can come to complete halt.

You can protect your network from broadcast storms by setting a port or trunk threshold for broadcast traffic. Any broadcast packets exceeding the specified threshold will then be dropped.

Command Usage

- Broadcast Storm Control is enabled by default.
- The default threshold is six percent of the port bandwidth.
- Broadcast control does not effect IP multicast traffic.

Command Attributes

- **Type** – Indicates the port type (100BASE-TX, 1000BASE-T, 1000BASE-SX, 1000BASE-LX or 100BASE-FX).
- **Protect Status** – Shows whether or not broadcast storm control has been enabled on this interface. (Default: Enabled)
- **Threshold** – Threshold as percentage of port bandwidth. (Options: 6%, 20%; Default: 6%)
- **Trunk** – Indicates if a port is a member of a trunk. To create trunks and select port members, see “Port Trunk Configuration” on page 2-79.

Web – Click Port, Port Broadcast Control or Trunk Broadcast Control. Set the threshold for each port or trunk, and then click **Apply**.

Port Broadcast Control

| Port | Type | Protect Status | Threshold (6% or 20%) | Trunk |
|------|------------|--|--------------------------------|--------------------------|
| 1 | 100Base-TX | <input checked="" type="checkbox"/> Enable | <input type="text" value="6"/> | <input type="checkbox"/> |
| 2 | 100Base-TX | <input checked="" type="checkbox"/> Enable | <input type="text" value="6"/> | <input type="checkbox"/> |
| 3 | 100Base-TX | <input checked="" type="checkbox"/> Enable | <input type="text" value="6"/> | <input type="checkbox"/> |
| 4 | 100Base-TX | <input checked="" type="checkbox"/> Enable | <input type="text" value="6"/> | <input type="checkbox"/> |
| 5 | 100Base-TX | <input checked="" type="checkbox"/> Enable | <input type="text" value="6"/> | <input type="checkbox"/> |
| 6 | 100Base-TX | <input checked="" type="checkbox"/> Enable | <input type="text" value="6"/> | <input type="checkbox"/> |

CLI – Specify an interface, and then enter the threshold. The following sets broadcast suppression at twenty percent of the port bandwidth for Port 3.

| | |
|---|---|
| <pre> Console(config)#interface ethernet 1/3 Console(config-if)#switchport broadcast percent 20 Console(config-if)#end Console#show interface switchport ethernet 1/3 Information of Eth 1/3 Broadcast threshold: Enabled, 20 percent Ingress rate limit: Disabled Egress rate limit: Disabled VLAN membership mode: Access Ingress rule: Disabled Acceptable frame type: All frames Native VLAN: 1 Priority for untagged traffic: 0 Gvrp status: Disabled Allowed Vlan: 1(u), Forbidden Vlan: Private-vlan mode: NONE Private-vlan host-association: NONE Private-vlan mapping: NONE Console# </pre> | <p>3-89</p> <p>3-97</p> <p>3-102</p> |
|---|---|

Configuring Port Mirroring

You can mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner.

Command Usage

- Monitor port speed should match or exceed source port speed, otherwise traffic may be dropped from the monitor port.
- All mirror sessions have to share the same destination port.
- When mirroring port traffic, the target port must be included in the same VLAN as the source port.
- The switch can only mirror one port at a time.

Command Attributes

- **Mirror Sessions** – Displays a list of current mirror sessions.
- **Source Port** – The port whose traffic will be monitored.
- **Type** – Allows you to select which traffic to mirror to the target port, Rx (receive), Tx (transmit), or Both.
- **Target Port** – The port that will “duplicate” or “mirror” the traffic on the source port.

Web – Click Port, Mirror. Specify the source port, the traffic type to be mirrored, and the monitor port, then click **Add**.

Mirror Port Configuration

Mirror Sessions:

Source: 1/10 Rx Destination: 1/13

<<Add

Remove

New:

Source Port

8

Type

Rx

Target Port

8

CLI – Use the interface command to select the monitor port, then use the port monitor command to specify the source port. Note that default mirroring under the CLI is for both received and transmitted packets.

Console(config)#interface ethernet 1/10

Console(config-if)#port monitor ethernet 1/13

Console(config-if)#

3-89

3-148

Address Table Settings

Switches store the addresses for all known devices. This information is used to route traffic directly between the inbound and outbound ports. All the addresses learned by monitoring traffic are stored in the dynamic address table. You can also manually configure static addresses that are bound to a specific port.

Setting Static Addresses

A static address can be assigned to a specific interface on this switch. Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.

Command Attributes

- **Static Address Counts*** – The number of manually configured addresses.
- **Current Static Address Table** – Lists all the static addresses.
- **Mode** – Indicates if a packet with a destination address matching an entry in the static address table will be forwarded or discarded.
- **Interface** – Port or trunk associated with the device assigned a static address.
- **MAC Address** – Physical address of a device mapped to this interface.
- **Duration** – The address can be set to the following type:
 - **Permanent** - Assignment is permanent, and restored after the switch is reset.
 - **Delete on Reset** - Assignment lasts until the switch is reset.

*Web Only

Web – Click Address Table, Static Addresses. Specify the mode, the interface, the MAC address and duration, then click Add Static Address.

The screenshot shows a web interface window titled "Static Addresses". It contains a form with the following fields and controls:

- Static Address Counts:** A text input field containing the number "1".
- Current Static Address Table:** A text area displaying "00-E0-29-94-34-DE, Unit 1, Port 3, Permanent".
- Mode:** A dropdown menu set to "Forward".
- Interface:** Two dropdown menus. The first is set to "Port 1" (with a radio button icon) and the second is set to "Trunk 1" (with a radio button icon).
- MAC Address:** An empty text input field.
- Duration:** A dropdown menu set to "Delete on Reset".
- Buttons:** Two buttons at the bottom: "Add Static Address" and "Remove Static Address".

CLI – This example adds an address to the static address table, and sets it to permanent by default.

```
Console(config)#mac-address-table static 00-e0-29-94-34-de  
interface ethernet 1/3  
Console(config)#
```

3-107

Displaying the Address Table

The Dynamic Address Table contains the MAC addresses learned by monitoring the source address for traffic entering the switch. When the destination address for inbound traffic is found in the database, the packets intended for that address are forwarded directly to the associated port. Otherwise, the traffic is flooded to all ports.

Command Attributes

- **Interface** – Indicates a port or trunk.
- **MAC Address** – Physical address associated with this interface.
- **Address Table Sort Key** – You can sort the information displayed based on interface (port or trunk) or MAC address.

Web – Click Address Table, Dynamic Addresses. Specify the search type (i.e. mark the Interface or MAC Address checkbox), select the method of sorting the displayed addresses, and then click **Query**.

Dynamic Addresses

Query by:

☐ Interface

☒ Port 1
 ☐ Trunk

☐ MAC Address

Address Table Sort Key

Address

Query

CLI – This example also displays the address table entries for port 1.

```

Console#sh mac-address-table ethernet 1/1 sort address
Mac Address      Interface Type
-----
00-10-B5-62-03-74  Eth 1/ 1 Learned
Console#
  
```

Changing the Aging Time

You can set the aging time for entries in the dynamic address table.

Command Attributes

- **Aging Time** – The time after which a learned entry is discarded.
(Range: 2-172800 seconds; Default: 300 seconds)

Web – Click Address Table, Address Aging. Specify the new aging time, click **Apply**.



CLI – This example sets the aging time to 400 seconds.

```
Console(config)#mac-address-table aging-time 400
```

3-110

Spanning Tree Algorithm Configuration

The Spanning Tree Algorithm (STA) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STA-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

STA uses a distributed algorithm to select a bridging device (STA-compliant switch, bridge or router) that serves as the root of the spanning tree network. It selects a root port on each bridging

device (except for the root device) which incurs the lowest path cost when forwarding a packet from that device to the root device. Then it selects a designated bridging device from each LAN which incurs the lowest path cost when forwarding a packet from that LAN to the root device. All ports connected to designated bridging devices are assigned as designated ports. After determining the lowest cost spanning tree, it enables all root ports and designated ports, and disables all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops.

Managing Global Settings

Global settings apply to the entire switch.

Command Attributes

The following global attributes are fixed and cannot be changed:

- **Bridge ID** – The priority and MAC address of this device.
- **Designated Root** – The priority and MAC address of the device in the Spanning Tree that this switch has accepted as the root device.
- **Root Port** – The number of the port on this switch that is closest to the root. This switch communicates with the root device through this port. If there is no root port, then this switch has been accepted as the root device of the Spanning Tree network.
- **Root Path Cost** – The path cost from the root port on this switch to the root device.

The following global attributes display statistical values and cannot be changed:

- **Configuration Changes** – The number of times the Spanning Tree has been reconfigured.
- **Last Topology Change** – Time since the Spanning Tree was last reconfigured.

The following global attributes can be configured:

- **Spanning Tree State** – Enables/disables this switch to participate in a STA-compliant network.
- **Priority** – Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device. (Note that lower numeric values indicate higher priority.)
 - Default: 32768
 - Range: 0 - 65535
- **Hello Time** – Interval (in seconds) at which the root device transmits a configuration message.
 - Default: 2
 - Minimum: 1
 - Maximum: The lower of 10 or [(Max. Message Age / 2) - 1]
- **Maximum Age** – The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to

the network. (References to “ports” in this section means “interfaces,” which includes both ports and trunks.)

- Default: 20
- Minimum: The higher of 6 or $[2 \times (\text{Hello Time} + 1)]$.
- Maximum: The lower of 40 or $[2 \times (\text{Forward Delay} - 1)]$
- **Forward Delay** – The maximum time (in seconds) the root device will wait before changing states (i.e., listening to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result.
 - Default: 15
 - Minimum: The higher of 4 or $[(\text{Max. Message Age} / 2) + 1]$
 - Maximum: 30

Displaying the Global Settings for STA

Web – Click Spanning Tree, STA Information.

| STA Information | | | |
|---------------------|--------------------|-----------------------|--------------------|
| Spanning Tree: | | | |
| Spanning Tree State | Enabled | Designated Root | 32768.0030F154F880 |
| Bridge ID | 32768.0055FFFFDDDD | Root Port | 2 |
| Max Age | 20 | Root Path Cost | 18 |
| Hello Time | 2 | Configuration Changes | 5 |
| Forward Delay | 15 | Last Topology Change | 0 d 1 h 57 min 5 s |

CLI – This command displays global STA settings, followed by settings for each port.

```

Console#show spanning-tree                                     3-119
Bridge-group information
-----
Spanning tree protocol           :IEEE Std 8021D
Spanning tree enable/disable    :enable
Priority                         :32768
Hello Time (sec.)               :2
Max Age (sec.)                  :20
Forward Delay (sec.)            :15
Designated Root                 :32768.0030f147583a
Current root port                :0
Current root cost                :0
Number of topology changes      :1
Last topology changes time (sec.):26696
Hold times (sec.)               :1
-----
Eth 1/ 1 information
-----
Admin status                    : enable
STA state                       : broken
Path cost                       : 18
Priority                         : 128
Designated cost                 : 0
Designated port                 : 128.1
Designated root                 : 32768.0030f147583a
Designated bridge               : 32768.0030f147583a
Fast forwarding                 : disable
Forward transitions              : 0
.
.
.

```

Note: The current root port and current root cost display as zero when this device is not connected to the network.

Configuring the Global Settings for STA

Web – Click Spanning Tree, STA Configuration. Modify the required attributes, and click Apply.

STA Configuration

Switch:

| | |
|---------------------|---------|
| Spanning Tree State | Enabled |
| Priority | 40000 |

When the Switch Becomes Root:

| | | |
|---------------------|----|---------|
| Hello Time(1-10) | 5 | seconds |
| Maximum Age(6-40) | 40 | seconds |
| Forward Delay(4-30) | 20 | seconds |

CLI – This example enables Spanning Tree Protocol, and then sets the indicated attributes.

| | |
|---|-------|
| Console(config)#spanning-tree | 3-112 |
| Console(config)#spanning-tree priority 40000 | 3-116 |
| Console(config)#spanning-tree hello-time 5 | 3-114 |
| Console(config)#spanning-tree max-age 38 | 3-115 |
| Console(config)#spanning-tree forward-time 20 | 3-113 |
| Console(config)# | |

Managing STA Interface Settings

You can configure STA attributes for specific interfaces, including port priority, path cost, and fast forwarding. You may use a different priority or path cost for ports of same media type to indicate the preferred path.

Command Attributes

The following attributes are read-only and cannot be changed:

- **Port Status** – Displays current state of this port within the Spanning Tree:
 - **Disabled** - The port has been disabled by the user or has failed diagnostics.
 - **Blocking** - Port receives STA configuration messages, but does not forward packets.
 - **Listening** - Port will leave blocking state due to a topology change, start transmitting configuration messages, but does not yet forward packets.
 - **Learning** - Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.
 - **Forwarding** - Port forwards packets, and continues learning addresses.
 - **Broken** - Port is malfunctioning or no link has been established.

The rules defining port status are:

- A port on a network segment with no other STA compliant bridging device is always forwarding.
- If two ports of a switch are connected to the same segment and there is no other STA device attached to this segment, the port with the smaller ID forwards packets and the other is blocked.
- All ports are blocked when the switch is booted, then some of them change state to listening, to learning, and then to forwarding.
- **Forward Transitions** – The number of times this port has transitioned from the Learning state to the Forwarding state.

- **Designated Cost** – The cost for a packet to travel from this port to the root in the current Spanning Tree configuration. The slower the media, the higher the cost.
- **Designated Bridge** – The priority and MAC address of the device through which this port must communicate to reach the root of the Spanning Tree.
- **Designated Port** – The priority and number of the port on the designated bridging device through which this switch must communicate with the root of the Spanning Tree.
- **Trunk Member** – Indicates if a port is a member of a trunk. (STA Port Information only)

The following interface attributes can be configured:

- **Priority** – Defines the priority used for this port in the Spanning Tree Protocol. If the path cost for all ports on a switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Protocol is detecting network loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.
 - Default: 128
 - Range: 0 - 255

- **Path Cost** – This parameter is used by the STP to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.)
 - Full Range: 1-65535
 - Recommended Range –
 - Ethernet: 50-600
 - Fast Ethernet: 10-6
 - Gigabit Ethernet: 3-10
 - Defaults –
 - Ethernet – half duplex: 100; full duplex: 95; trunk: 90
 - Fast Ethernet – half duplex: 19; full duplex: 18; trunk: 15
 - Gigabit Ethernet – full duplex: 4; trunk: 3
- **Fast Forwarding** – You can enable this option if an interface is attached to a LAN segment that is at the end of a bridged LAN or to an end node. Since end-nodes cannot cause forwarding loops, they can pass directly through to the forwarding state. Fast Forwarding can achieve quicker convergence for end-node workstations and servers, and also overcome other STA related timeout problems. (Remember that Fast Forwarding should only be enabled for ports connected to an end-node device.)
 - Default: disabled

Displaying the Interface Settings for STA

Web – Click Spanning Tree, STA Port Information or STA Trunk Information.

| STA Port Information | | | | | | |
|----------------------|-------------|---------------------|-----------------|--------------------|-----------------|--------------|
| Port | Port Status | Forward Transitions | Designated Cost | Designated Bridge | Designated Port | Trunk Member |
| 1 | Forwarding | 2 | 18 | 32768.0055FFFFDDDD | 128.1 | |
| 2 | Forwarding | 2 | 0 | 32768.0030F154F880 | 128.11 | |
| 3 | Broken | 0 | 18 | 32768.0055FFFFDDDD | 128.3 | |
| 4 | Broken | 0 | 18 | 32768.0055FFFFDDDD | 128.4 | |
| 5 | Broken | 0 | 18 | 32768.0055FFFFDDDD | 128.33 | 1 |
| 6 | Broken | 0 | 18 | 32768.0055FFFFDDDD | 128.6 | |

CLI – This example shows the STA attributes for port 5.

```

Console#show spanning tree ethernet 1/5
Bridge-group information
-----
Spanning tree protocol           :IEEE Std 802.1D
Spanning tree enable/disable    :enable
Priority                         :32768
Hello Time (sec.)               :2
Max Age (sec.)                  :20
Forward Delay (sec.)            :15
Designated Root                  :32768.0030F154F880
Current root port                :2
Current root cost                :18
Number of topology changes      :5
Last topology changes time (sec.):12828
Hold times (sec.)               :1
-----

Eth 1/ 1 information
-----
Admin status                    : enable
STA state                       : forwarding
Path cost                       : 18
Priority                         : 128
Designated cost                  : 18
Designated port                  : 128.1
Designated root                  : 32768.0030F154F880
Designated bridge                : 32768.0055FFFFDDDD
Fast forwarding                  : disable
Forward transitions              : 2
Console#
  
```

Configuring the Interface Settings for STA

Web – Click Spanning Tree, STA Port Configuration or STA Trunk Configuration. Modify the required attributes, then click Apply.

| STA Port Configuration | | | | | | |
|------------------------|------------|------------|----------|-----------|---|-------|
| Port | Type | STA State | Priority | Path Cost | Fast Forwarding | Trunk |
| 1 | 100Base-TX | Forwarding | 0 | 50 | <input checked="" type="checkbox"/> Enabled | |
| 2 | 100Base-TX | Forwarding | 128 | 18 | <input type="checkbox"/> Enabled | |
| 3 | 100Base-TX | Broken | 128 | 100 | <input type="checkbox"/> Enabled | |
| 4 | 100Base-TX | Broken | 128 | 100 | <input type="checkbox"/> Enabled | |
| 5 | 100Base-TX | Broken | 128 | 90 | <input checked="" type="checkbox"/> Enabled | 1 |
| 6 | 100Base-TX | Broken | 128 | 100 | <input type="checkbox"/> Enabled | |

CLI – This example sets STA attributes for port 5.

| | |
|--|-------|
| Console(config)#interface ethernet 1/5 | 3-89 |
| Console(config-if)#spanning-tree port-priority 0 | 3-117 |
| Console(config-if)#spanning-tree cost 50 | 3-116 |
| Console(config-if)#spanning-tree portfast | 3-118 |

VLAN Configuration

In conventional networks with routers, broadcast traffic is split up into separate domains. Switches do not inherently support broadcast domains. This can lead to broadcast storms in large networks that handle traffic such as IPX or NetBeui. By using IEEE 802.1Q-compliant VLANs, you can organize any group of network nodes into separate broadcast domains, thus confining broadcast traffic to the originating group. This also provides a more secure and cleaner network environment.

An IEEE 802.1Q VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment.

VLANs help to simplify network management by allowing you to move devices to a new VLAN without having to change any physical connections. VLANs can be easily organized to reflect departmental groups (such as Marketing or R&D), usage groups (such as e-mail), or multicast groups (used for multimedia applications such as videoconferencing).

VLANs provide greater network efficiency by reducing broadcast traffic, and allow you to make network changes without having to update IP addresses or IP subnets. VLANs inherently provide a high level of network security since traffic must pass through a configured Layer 3 link to reach a different VLAN.

This switch supports the following VLAN features:

- Up to 127 VLANs based on the IEEE 802.1Q standard
- Distributed VLAN learning across multiple switches using explicit or implicit tagging and GVRP protocol
- Port overlapping, allowing a port to participate in multiple VLANs
- End stations can belong to multiple VLANs
- Passing traffic between VLAN-aware and VLAN-unaware devices
- Priority tagging

Assigning Ports to VLANs

Before enabling VLANs for the switch, you must first assign each port to the VLAN group(s) in which it will participate. By default all ports are assigned to VLAN 1 as untagged ports. Add a port as a tagged port if you want it to carry traffic for one or more VLANs, and any intermediate network devices or the host at the other end of the connection supports VLANs. Then assign ports on the other VLAN-aware network devices along the path that will carry this

traffic to the same VLAN(s), either manually or dynamically using GVRP. However, if you want a port on this switch to participate in one or more VLANs, but none of the intermediate network devices nor the host at the other end of the connection supports VLANs, then you should add this port to the VLAN as an untagged port.

Note: VLAN-tagged frames can pass through VLAN-aware or VLAN-unaware network interconnection devices, but should not be used for any end-node host that does not support VLAN tagging.

VLAN Classification – When the switch receives a frame, it classifies the frame in one of two ways. If the frame is untagged, the switch assigns the frame to an associated VLAN (based on the PVID of the receiving port). But if the frame is tagged, the switch uses the tagged VLAN ID to identify the port broadcast domain of the frame.

Port Overlapping – Port overlapping can be used to allow access to commonly shared network resources among different VLAN groups, such as file servers or printers. Note that if you implement VLANs which do not overlap, but still need to communicate, you can connect them by using a Layer-3 router or switch.

Untagged VLANs – Untagged (or static) VLANs are typically used to reduce broadcast traffic and to increase security. A group of network users assigned to a VLAN form a broadcast domain that is separate from other VLANs configured on the switch. Packets are forwarded only between ports that are designated for the same VLAN. Untagged VLANs can be used to manually isolate user groups or subnets. However, you should use IEEE 802.3 tagged VLANs with GVRP whenever possible to fully automate VLAN registration.

Automatic VLAN Registration – GVRP (GARP VLAN Registration Protocol) defines a system whereby the switch can automatically learn the VLANs to which each endstation should be assigned. If an endstation (or its network adapter) supports the IEEE 802.1Q VLAN protocol, it can be configured to broadcast a message to your network indicating the VLAN groups it wants to join. When this switch receives these messages, it will automatically place the receiving port in the specified VLANs, and then forward the message to all other ports. When the message arrives at another switch that supports GVRP, it will also place the receiving port in the specified VLANs, and pass the message on to all other ports. VLAN requirements are propagated in this way throughout the network. This allows GVRP-compliant devices to be automatically configured for VLAN groups based solely on endstation requests.

To implement GVRP in a network, first add the host devices to the required VLANs (using the operating system or other application software), so that these VLANs can be propagated onto the network. For both the edge switches attached directly to these hosts, and core switches in the network, enable GVRP on the links between these devices. You should also determine security boundaries in the network and disable GVRP on ports to prevent advertisements being propagated, or forbid ports from joining restricted VLANs.

Note: If you have host devices that do not support GVRP, you must configure static VLANs for the switch ports connected to these devices (as described in “Adding Static Members to VLANs (VLAN Index)” on page 2-61). But you still need to enable GVRP on these edge switches, as well as on the core switches in the network.

Forwarding Tagged/Untagged Frames

If you want to create a small port-based VLAN for devices attached directly to a single switch, you can assign ports to the same untagged VLAN. However, to participate in a VLAN group that crosses several switches, you need to create a VLAN for that group and enable tagging on all ports.

Ports can be assigned to multiple tagged or untagged VLANs. Each port on the switch is therefore capable of passing tagged or untagged frames. When forwarding a frame from this switch along a path that contains any VLAN-aware devices, the switch should include VLAN tags. When forwarding a frame from this switch along a path that does not contain any VLAN-aware devices (including the destination host), the switch must first strip off the VLAN tag before forwarding the frame. When the switch receives a tagged frame, it will pass this frame onto the VLAN(s) indicated by the frame tag. However, when this switch receives an untagged frame from a VLAN-unaware device, it first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port's default VID.

Displaying Basic VLAN Information

The VLAN Basic Information page displays basic information on the VLAN type supported by the switch.

Command Attributes

- **VLAN Version Number*** – The VLAN version used by this switch as specified in the IEEE 802.1Q standard.
- **Maximum VLAN ID** – Maximum VLAN ID recognized by this switch.
- **Maximum Number of Supported VLANs** – Maximum number of VLANs that can be configured on this switch.

*Web Only

Web – Click VLAN, VLAN Base Information.

| VLAN Basic Information | |
|-----------------------------------|------|
| VLAN Version Number | 1 |
| Maximum VLAN ID | 4094 |
| Maximum Number of Supported VLANs | 127 |

CLI – Enter the following command.

```

Console#show bridge-ext
Max support vlan numbers: 127
Max support vlan ID: 4094
Extended multicast filtering services: No
Static entry individual port: Yes
VLAN learning: SVL
Configurable PVID tagging: Yes
Local VLAN capable: No
Traffic classes: Enabled
Global GVRP status: Enabled
GMRP: Disabled
Console#
    
```

3-145

Displaying Current VLANs

The VLAN Current Table shows the current port members of each VLAN and whether or not the port supports VLAN tagging. Ports assigned to a large VLAN group that crosses several switches should use VLAN tagging. However, if you just want to create a small port-based VLAN for one or two switches, you can disable tagging.

Command Attributes (Web)

- **VLAN ID** – ID of configured VLAN (1-4094, no leading zeroes).
- **Up Time at Creation** – Time this VLAN was created (i.e., System Up Time).

- **Status** – Shows how this VLAN was added to the switch.
 - **Dynamic GVRP**: Automatically learned via GVRP.
 - **Permanent**: Added as a static entry.
- **Egress Ports** – Shows all the VLAN port members.
- **Untagged Ports** – Shows the untagged VLAN port members.

Web – Click VLAN, VLAN Current Table. Select any ID from the scroll-down list.

VLAN Current Table

VLAN ID:

Up Time at Creation: 0 d 0 h 0 min 7 s

Status: Permanent

| Egress Ports | Untagged Ports |
|--------------|----------------|
| Unit1 Port1 | Unit1 Port1 |
| Unit1 Port2 | Unit1 Port2 |
| Unit1 Port3 | Unit1 Port3 |
| Unit1 Port4 | Unit1 Port4 |
| Unit1 Port6 | Unit1 Port6 |
| Unit1 Port7 | Unit1 Port7 |
| Unit1 Port8 | Unit1 Port8 |
| Unit1 Port9 | Unit1 Port9 |

Command Attributes (CLI)

- **VLAN** – ID of configured VLAN (1-4094, no leading zeroes).
- **Type** – Shows how this VLAN was added to the switch.
 - **Dynamic**: Automatically learned via GVRP.
 - **Static**: Added as a static entry.
- **Name** – Name of the VLAN (1 to 32 characters).
- **Status** – Shows if this VLAN is enabled or disabled.
 - **Active**: VLAN is operational.
 - **Suspend**: VLAN is suspended; i.e., does not pass packets.

- **Ports / Channel groups** – Shows the VLAN interface members.

CLI – Current VLAN information can be displayed with the following command.

| Console#show vlan id 1 | | | | 3-131 | | | |
|------------------------|--------|-------------|--------|----------------------|---------|---------|---------|
| VLAN | Type | Name | Status | Ports/Channel groups | | | |
| 1 | Static | DefaultVlan | Active | Eth1/1 | Eth1/2 | Eth1/3 | Eth1/4 |
| | | | | Eth1/5 | Eth1/6 | Eth1/7 | Eth1/8 |
| | | | | Eth1/9 | Eth1/10 | Eth1/11 | Eth1/12 |
| | | | | Eth1/13 | Eth1/14 | Eth1/15 | Eth1/16 |
| | | | | Eth1/17 | Eth1/18 | Eth1/19 | Eth1/20 |
| | | | | Eth1/21 | Eth1/22 | Eth1/23 | Eth1/24 |
| Console# | | | | | | | |

Creating VLANs

Use the VLAN Static List to create or remove VLAN groups. To propagate information about VLAN groups used on this switch to external network devices, you must specify a VLAN ID for each of these groups.

Command Attributes

- **Current** – Lists all the current VLAN groups created for this system. Up to 127 VLAN groups can be defined. VLAN 1 is the default untagged VLAN.
- **New** – Allows you to specify the name and numeric identifier for a new VLAN group. (The VLAN name is only used for management on this system; it is not added to the VLAN tag.)
- **VLAN ID** – ID of configured VLAN (1-4094, no leading zeroes).
- **VLAN Name** – Name of the VLAN (1 to 32 characters).
- **Status** (Web) – Shows if this VLAN is enabled or disabled.
 - **Enable:** VLAN is operational.
 - **Disable:** VLAN is suspended; i.e., does not pass packets.

- **State** (CLI) – Shows if this VLAN is enabled or disabled.
 - **Active:** VLAN is operational.
 - **Suspend:** VLAN is suspended; i.e., does not pass packets.
- **Add** – Adds a new VLAN group to the current list.
- **Remove** – Removes a VLAN group from the current list. If any port is assigned to this group as untagged, it will be reassigned to VLAN group 1 as untagged.

Web – Click VLAN, VLAN Static List. To create a new VLAN, enter the VLAN ID and VLAN name, mark the Enable checkbox to activate the VLAN, and then click Add.

VLAN Static List

Current:

1, DefaultVlan, Enabled

New:

VLAN ID (1-4094)2

VLAN NameR&D

Status☒ Enable

<<Add

Remove

CLI – This example creates a new VLAN.

```

Console(config)#vlan database
Console(config-vlan)#vlan 2 name R&D media ethernet state active
3-123
Console(config-vlan)#end
Console#show vlan
VLAN  Type      Name           Status      Ports/Channel groups
-----
1   Static   DefaultVlan    Active      Eth1/ 1 Eth1/ 2 Eth1/ 3
                                           Eth1/ 4 Eth1/ 5 Eth1/ 6
                                           Eth1/ 7 Eth1/ 8 Eth1/ 9
                                           Eth1/10 Eth1/11 Eth1/12
                                           Eth1/13 Eth1/14 Eth1/15
                                           Eth1/16 Eth1/17 Eth1/18
                                           Eth1/19 Eth1/20 Eth1/21
                                           Eth1/22 Eth1/23 Eth1/24
2   Static   R&D            Active
Console#
    
```

Adding Static Members to VLANs (VLAN Index)

Use the VLAN Static Table to configure port members for the selected VLAN index. Assign ports as tagged if they are connected to 802.1Q VLAN compliant devices, or untagged they are not connected to any VLAN-aware devices. Or configure a port as forbidden to prevent the switch from automatically adding it to a VLAN via the GVRP protocol.

- Notes:**
1. You can also use the VLAN Static Membership by Port page to configure VLAN groups based on the port index. However, note that this configuration page can only add ports to a VLAN as tagged members.
 2. VLAN 1 is the default untagged VLAN containing all ports on the switch, and can only be modified by first reassigning the default port VLAN ID as described under “Configuring VLAN Behavior for Interfaces” on page 2-65.

Command Attributes

- **VLAN** – ID of configured VLAN (1-4094, no leading zeroes).
- **Name** – Name of the VLAN (1 to 32 characters).
- **Status** – Shows if this VLAN is enabled or disabled.
 - **Enable:** VLAN is operational.
 - **Disable:** VLAN is suspended; i.e., does not pass packets.
- **Port** – Port identifier.
- **Trunk** – Trunk identifier.

- **Membership Type** – Select VLAN membership for each interface by marking the appropriate radio button for a port or trunk:
 - **Tagged:** Interface is a member of the VLAN. All packets transmitted by the port will be tagged, that is, carry a tag and therefore carry VLAN or CoS information.
 - **Untagged:** Interface is a member of the VLAN. All packets transmitted by the port will be untagged, that is, not carry a tag and therefore not carry VLAN or CoS information. Note that an interface must be assigned to at least one group as an untagged port.
 - **Forbidden:** Interface is forbidden from automatically joining the VLAN via GVRP.
 - **None:** Interface is not a member of the VLAN. Packets associated with this VLAN will not be transmitted by the interface.
- **Trunk Member** – Indicates if a port is a member of a trunk. To add a trunk to the selected VLAN, use the last table on the VLAN Static Table page.

Web – Click VLAN, VLAN Static Table. Select a VLAN ID from the scroll-down list. Modify the VLAN name and status if required. Select the membership type by marking the appropriate radio button in the list of ports or trunks. Click Apply.

VLAN Static Table

VLAN: 1

Name
DefaultVlan

Status
☒ Enable

| Port | Member | Forbidden | None | Trunk Member |
|------|----------------------------------|-----------------------|-----------------------|--------------|
| 1 | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> | |
| 2 | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> | |
| 3 | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> | |
| 4 | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> | |
| 5 | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> | |

CLI – This example adds the required interfaces.

```

Console(config)#interface ethernet 1/1                               3-89
Console(config-if)#switchport allowed vlan add 2 tagged            3-129
Console(config-if)#exit
Console(config)#interface ethernet 1/2
Console(config-if)#switchport allowed vlan add 2 untagged
Console(config-if)#exit
Console(config)#interface ethernet 1/13
Console(config-if)#switchport forbidden vlan add 2                 3-130

```

Adding Static Members to VLANs (Port Index)

Use the VLAN Static Membership by Port menu to assign VLAN groups to the selected interface add an interface to the selected VLAN as a tagged member.

Command Attributes

- **Interface** – Port or trunk identifier.
- **Member** – VLANs for which the selected interface is a tagged member.
- **Non-Member** – VLANs for which the selected interface is not a member.

Web – Click VLAN, VLAN Static Membership by Port. Select an interface from the scroll-down box (Port or Trunk). Click Query to display membership information for the interface. Select a VLAN ID, and then click Add to add the interface as a tagged member, or click Remove to remove the interface. After configuring VLAN membership for each interface, click Apply.

The screenshot shows a web interface titled "VLAN Static Membership by Port". At the top, there is a section for "Interface" with two dropdown menus: "Port" (selected) and "Trunk" (selected). Below this is a "Query" button. Underneath, there are two lists: "Member:" and "Non-Member:". The "Member:" list contains "Vlan 1". The "Non-Member:" list contains "Vlan 2". Between these two lists are two buttons: "<< Add" and "Remove >>".

CLI – This example adds Port 3 to VLAN 1 as a tagged port.

| | |
|---|-------|
| Console(config)#interface ethernet 1/3 | 3-89 |
| Console(config-if)#switchport allowed vlan add 1 tagged | 3-129 |

Configuring VLAN Behavior for Interfaces

You can configure VLAN behavior for specific interfaces, including the default VLAN identifier (PVID), accepted frame types, ingress filtering, GVRP status, and GARP timers.

Command Usage

- **GVRP** – GARP VLAN Registration Protocol defines a way for switches to exchange VLAN information in order to automatically register VLAN members on interfaces across the network.
- **GARP** – Group Address Registration Protocol is used by GVRP to register or deregister client attributes for client services within a bridged LAN. The default values for the GARP timers are independent of the media access method or data rate. These values should not be changed unless you are experiencing difficulties with GVRP registration/deregistration.

Command Attributes

- **Ingress Filtering** – If ingress filtering is enabled, incoming frames for VLANs which do not include this ingress port in their member set will be discarded at the ingress port. (Default: Disabled)
 - Ingress filtering only affects tagged frames.
 - If ingress filtering is disabled, the interface will accept any VLAN-tagged frame if the tag matches a VLAN known to the switch (except for those VLANs explicitly forbidden on this port).

- If ingress filtering is enabled, the interface will discard incoming frames tagged for VLANs which do not include this ingress port in their member set.
- Ingress filtering does not affect VLAN independent BPDU frames, such as GVRP or STP. However, it does affect VLAN dependent BPDU frames, such as GMRP.
- **PVID** – VLAN ID assigned to untagged frames received on the interface. (Default: 1)
 - If an interface is not a member of VLAN 1 and you assign its PVID to this VLAN, the interface will automatically be added to VLAN 1 as an untagged member. For all other VLANs, an interface must first be configured as an untagged member before you can assign its PVID to that group.
- **Acceptable Frame Type** – Sets the interface to accept all frame types, including tagged or untagged frames, or only tagged frames. When set to receive all frame types, any received frames that are untagged are assigned to the default VLAN. (Option: All, Tagged; Default: All)
 - This field is read-only for the Web, and read/write for the CLI (page 3-126).
- **GVRP Status** – Enables/disables GVRP for the interface. GVRP must be globally enabled for the switch before this setting can take effect. (See “Displaying Bridge Extension Capabilities” on page 2-24.) When disabled, any GVRP packets received on this port will be discarded and no GVRP registrations will be propagated from other ports. (Default: Disabled)
 - GVRP can only be enabled for tagged ports.
 - You must set Mode to 1Q Trunk to configure a tagged port.
- **GARP Join Timer*** – The interval between transmitting requests/queries to participate in a VLAN group. (Range: 20-1000 centiseconds; Default: 20)

- **GARP Leave Timer*** – The interval a port waits before leaving a VLAN group. This time should be set to more than twice the join time. This ensures that after a Leave or LeaveAll message has been issued, the applicants can rejoin before the port actually leaves the group. (Range: 60-3000 centiseconds; Default: 60)
- **GARP LeaveAll Timer*** – The interval between sending out a LeaveAll query message for VLAN group participants and the port leaving the group. This interval should be considerably larger than the Leave Time to minimize the amount of traffic generated by nodes rejoining the group. (Range: 500-18000 centiseconds; Default: 1000)

*Timer settings must follow this rule:

$2 \times (\text{join timer}) < \text{leave timer} < \text{leaveAll timer}$

- **Trunk Member** – Indicates if a port is a member of a trunk. To add a trunk to the selected VLAN, use the last table on the VLAN Static Table page.
- **Mode** – Indicates VLAN membership egress mode for an interface. (Default: Access)
 - **Access** – Sets the port to operate as an untagged interface. All frames are sent untagged.
 - **1Q Trunk** – Specifies a port as an end-point for a VLAN trunk. A trunk is a direct link between two switches, so the port transmits tagged frames that identify the source VLAN. However, note that frames belonging to the port's default VLAN (i.e., associated with the PVID) are sent untagged.

Web – Click VLAN, VLAN Port Configuration or VLAN Trunk Configuration. Fill in the required settings for each interface, click Apply.

VLAN Port Configuration

Ingress Filtering

☐ Enabled

| Port | PVID | Acceptable Frame Type | GVRP Status | GARP Join Timer(Centi Seconds)(20-1000) | GARP Leave Timer(Centi Seconds)(60-3000) | GARP LeaveAll Timer(Centi Seconds)(500-18000) | Trunk Member | Mode |
|------|------|-----------------------|----------------------------------|---|--|---|--------------|----------|
| 1 | 1 | ALL | <input type="checkbox"/> Enabled | 20 | 60 | 1000 | | Access ▾ |
| 2 | 1 | ALL | <input type="checkbox"/> Enabled | 20 | 60 | 1000 | | Access ▾ |
| 3 | 1 | ALL | <input type="checkbox"/> Enabled | 20 | 60 | 1000 | | Access ▾ |

CLI – This example sets port 3 to accept only tagged frames, assigns PVID 2 as the native VLAN ID, enables GVRP, sets the GARP timers, and then sets the switchport mode to trunk.

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#switchport ingress-filtering
Console(config-if)#switchport native vlan 2
Console(config-if)#switchport gvrp
Console(config-if)#garp timer join 30
Console(config-if)#garp timer leave 90
Console(config-if)#garp timer leaveall 2000
Console(config-if)#switchport mode trunk
Console(config-if)#
```

3-89

3-126

3-127

3-128

3-140

3-142

3-142

3-142

3-125

Configuring Private VLANs

Private VLANs provide port-based security and isolation between ports within the assigned VLAN. This switch supports two types of private VLAN ports: promiscuous, and community ports. A promiscuous port can communicate with all interfaces within a private VLAN. Community ports can only communicate with other

ports in their own community VLAN, and with their designated promiscuous ports. (Note that private VLANs and normal VLANs can exist simultaneously within the same switch.)

Each private VLAN consists of two components: a primary VLAN and one or more community VLANs. A primary VLAN allows traffic to pass between promiscuous ports, and between promiscuous ports and community ports subordinate to the primary VLAN. A community VLAN conveys traffic between community ports, and from the community ports to their associated promiscuous ports. Multiple primary VLANs can be configured on this switch, and multiple community VLANs can be configured within each primary VLAN.

To configure private VLANs, follow these steps:

1. Use the Private VLAN Configuration menu (page 2-71) to designate one or more community VLANs and the primary VLAN that will channel traffic outside of the community groups.
2. Use the Private VLAN Association menu (page 2-72) to map the secondary (i.e., community) VLAN(s) to the primary VLAN.
3. Use the Private VLAN Port Configuration menu (page 2-75) to set the port type to promiscuous (i.e., having access to all ports in the primary VLAN) or host (i.e., having access restricted to community VLAN members, and channeling all other traffic through a promiscuous port). Then assign any promiscuous ports to a primary VLAN and any host ports a secondary VLAN (i.e., community VLAN).

Displaying Current Private VLANs

The Private VLAN Information page displays information on the private VLANs configured on the switch, including primary and community VLANs, and their associated interfaces.

Command Attributes

- **VLAN ID** – ID of configured VLAN (1-4094, no leading zeroes).
- **Primary VLAN** – The primary VLAN with which the selected VLAN is associated. (Note that this displays as VLAN 0 if the selected VLAN is itself a primary VLAN.)
- **Ports List** – The list of ports (and assigned type) in the selected private VLAN.

Web – Click Private VLAN, Private VLAN Information. Select the desired port from the VLAN ID drop-down menu.



The screenshot shows a web-based configuration interface titled "Private VLAN Information". It features a "VLAN ID:" label followed by a dropdown menu currently showing "5, Primary Vlan". Below this is a text box containing "Primary Vlan" and "Vlan 0". A section titled "Ports List" contains a scrollable area with three entries: "Unit 1, Port 3, Promiscuous", "Unit 1, Port 4, Host", and "Unit 1, Port 5, Host". The interface has a light gray border and a vertical scrollbar on the right side.

Private VLAN Information

VLAN ID: 5, Primary Vlan

Primary Vlan Vlan 0

Ports List

- Unit 1, Port 3, Promiscuous
- Unit 1, Port 4, Host
- Unit 1, Port 5, Host

CLI – This example shows the switch configured with primary VLAN 5 and secondary VLAN 6. Port 3 has been configured as a promiscuous port and mapped to VLAN 5, while ports 4 and 5 have been configured as a host ports and are associated with VLAN 6. This means that traffic for port 4 and 5 can only pass through port 3.

| Console#show vlan private-vlan | | | | 3-139 |
|--------------------------------|-----------|-----------|-----------------|-------|
| Primary | Secondary | Type | Interfaces | |
| ----- | ----- | ----- | ----- | |
| 5 | | primary | Eth1/ 3 | |
| 5 | 6 | community | Eth1/ 4 Eth1/ 5 | |
| Console# | | | | |

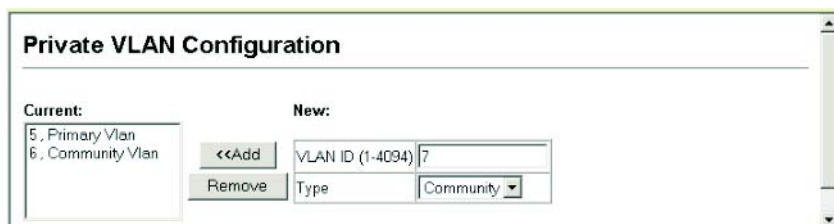
Configuring Private VLANs

The Private VLAN Configuration page is used to create/remove primary or community VLANs.

Command Attributes

- **VLAN ID** – ID of configured VLAN (1-4094, no leading zeroes).
- **Type** – There are two types of VLANs within a private VLAN:
 - **Primary VLANs** - Conveys traffic between promiscuous ports, and to community ports within secondary VLANs.
 - **Community VLANs** - Conveys traffic between community ports, and to their associated promiscuous ports.
- **Current** – Displays a list of the currently configured VLANs.

Web – Click Private VLAN, Private VLAN Configuration. Enter the VLAN ID number, select Primary or Community type, then click Add. To remove a private VLAN from the switch, highlight an entry in the Current list box and then click Remove. Note that all member ports must be removed from the VLAN before it can be deleted.



The screenshot shows the 'Private VLAN Configuration' web interface. It features a 'Current:' list box on the left containing '5, Primary Vlan' and '6, Community Vlan'. To the right of this list are 'Add' and 'Remove' buttons. Further right is a 'New:' section with a 'VLAN ID (1-4094)' input field containing the number '7', a 'Type' dropdown menu set to 'Community', and an 'Add' button. The interface has a light gray background and a white border.

CLI – This example configures VLAN 5 as a primary VLAN, and VLAN 6 and 7 as community VLANs.

```
Console(config)#vlan database
Console(config-vlan)#private-vlan 5 primary
Console(config-vlan)#private-vlan 6 community
Console(config-vlan)#private-vlan 7 community
Console(config-vlan)#
```

3-122
3-134

Associating Community VLANs

Each community VLAN must be associated with a primary VLAN.

Command Attributes

- **Primary VLAN ID** – ID of primary VLAN (1-4094, no leading zeroes).
- **Association** – Community VLANs associated with the selected primary VLAN.
- **Non-Association** – Community VLANs not associated with the selected primary VLAN.

Web – Click Private VLAN, Private VLAN Association. Select the required primary VLAN from the scroll-down box, highlight one or more community VLANs in the Non-Association list box, and click Add to associate these entries with the selected primary VLAN. (A community VLAN can only be associated with one primary VLAN.)

CLI – This example associates community VLANs 6 and 7 with primary VLAN 5.

| | |
|---|-------|
| Console(config)#vlan database | 3-122 |
| Console(config-vlan)#private-vlan 5 association 6 | 3-135 |
| Console(config-vlan)#private-vlan 5 association 7 | |
| Console(config)# | |

Displaying Private VLAN Interface Information

Use the Private VLAN Port Information and Private VLAN Trunk Information menus to display the interfaces associated with private VLANs.

Command Attributes

- **Port/Trunk** – The switch interface.
- **PVLAN Port Type** – Displays private VLAN port types.
 - **Normal** – The port is not configured in a private VLAN.
 - **Host** – The port is a community port and can only communicate with other ports in its own community VLAN, and with the designated promiscuous port(s).
 - **Promiscuous** – A promiscuous port can communicate with all the interfaces within a private VLAN.
- **Primary VLAN** – Conveys traffic between promiscuous ports, and between promiscuous ports and community ports within the associated secondary VLANs.
- **Secondary VLAN** – On this switch all secondary VLANs are community VLANs. A community VLAN conveys traffic between community ports, and from community ports to their designated promiscuous ports.
- **Trunk** – The trunk identifier. (Private VLAN Port Information only)

Web – Click Private VLAN, Private VLAN Port Information or Private VLAN Trunk Information.

| Private VLAN Port Information | | | | |
|-------------------------------|-----------------|--------------|----------------|-------|
| Port | PVLAN Port Type | Primary VLAN | Secondary VLAN | Trunk |
| 1 | Normal | | | |
| 2 | Normal | | | |
| 3 | Promiscuous | 5 | | |
| 4 | Host | | 6 | |
| 5 | Host | | 6 | |

CLI – This example shows the switch configured with primary VLAN 5 and secondary VLAN 6. Port 3 has been configured as a promiscuous port and mapped to VLAN 5, while ports 4 and 5 have been configured as a host ports and associated with VLAN 6. This means that traffic for port 4 and 5 can only pass through port 3.

| Console#show vlan private-vlan | | | | 3-139 |
|--------------------------------|-----------|-----------|-----------------|-------|
| Primary | Secondary | Type | Interfaces | |
| ----- | ----- | ----- | ----- | |
| 5 | | primary | Eth1/ 3 | |
| 5 | 6 | community | Eth1/ 4 Eth1/ 5 | |
| Console# | | | | |

Configuring Private VLAN Interfaces

Use the Private VLAN Port Configuration and Private VLAN Trunk Configuration menus to set the private VLAN interface type, and associate the interfaces with a private VLAN.

Command Attributes

- **Port/Trunk** – The switch interface.
- **PVLAN Port Type** – Sets the private VLAN port types.
 - **Normal** – The port is not configured into a private VLAN.
 - **Host** – The port is a community port and can only communicate with other ports in its own community VLAN, and with the designated promiscuous port(s).
 - **Promiscuous** – A promiscuous port can communicate with all interfaces within a private VLAN.

- **Primary VLAN** – Conveys traffic between promiscuous ports, and between promiscuous ports and community ports within the associated secondary VLANs. If PVLAN type is “Promiscuous,” then specify the associated primary VLAN. For “Host” type, the Primary VLAN displayed is the one to which the selected secondary VLAN has been associated.
- **Secondary VLAN** – On this switch, all secondary VLANs are community VLANs. A community VLAN conveys traffic between community ports, and from community ports to their designated promiscuous ports. If PVLAN Port Type is “Host,” then specify the associated secondary VLAN.

Web – Click Private VLAN, Private VLAN Port Configuration or Private VLAN Trunk Configuration. Set the PVLAN Port Type for each port that will join a private VLAN. For promiscuous ports, set the associated primary VLAN. For host ports, set the associated secondary VLAN. After all the ports have been configured, click Apply.

| Port | PVLAN Port Type | Primary VLAN | Secondary VLAN | Trunk |
|------|-----------------|--------------|----------------|-------|
| 1 | Normal | 5 | 6 | |
| 2 | Normal | 5 | 6 | |
| 3 | Promiscuous | 5 | 6 | |
| 4 | Host | 5 | 6 | |
| 5 | Host | 5 | 6 | |

CLI – This example shows the switch configured with primary VLAN 5 and secondary VLAN 6. Port 3 has been configured as a promiscuous port and mapped to VLAN 5, while ports 4 and 5 have been configured as a host ports and associated with VLAN 6. This means that traffic for port 4 and 5 can only pass through port 3.

| | |
|---|-------|
| Console(config)#interface ethernet 1/3 | 3-89 |
| Console(config-if)#switchport mode private-vlan promiscuous | 3-136 |
| Console(config-if)#switchport private-vlan mapping 5 | 3-138 |
| Console(config-if)#exit | |
| Console(config)#interface ethernet 1/4 | |
| Console(config-if)#switchport mode private-vlan host | 3-136 |
| Console(config-if)#switchport private-vlan host-association 6 | 3-137 |
| Console(config-if)#exit | |
| Console(config)#interface ethernet 1/5 | |
| Console(config-if)#switchport mode private-vlan host | |
| Console(config-if)#switchport private-vlan host-association 6 | |
| Console(config-if)# | |

Class of Service Configuration

Class of Service (CoS) allows data packets that have greater precedence to receive higher service priority when traffic is buffered in the switch due to congestion. This switch supports CoS with four priority queues for each port. Data packets in a port's high-priority queues will be transmitted before those in the lower-priority queues.

You can set the switch to service the queues based on a strict rule that requires all traffic in a higher priority queue to be processed before lower priority queues are serviced, or use Weighted Round-Robin (WRR) queuing that specifies a relative weight for each queue. WRR uses a predefined relative weight for each queue that determines the percentage of service time the switch services each queue before moving on to the next queue. This prevents the head-of-line blocking that can occur with strict priority queuing

This switch uses Weighted Round-Robin as the default mode for each port. Up to 8 separate traffic classes are defined in IEEE 802.1p. The default priority levels are assigned according to recommendations in the IEEE 802.1p standard as shown in the following table.

| | Queue | | | |
|----------|-------|---|---|---|
| | 0 | 1 | 2 | 3 |
| Priority | | 0 | | |
| | 1 | | | |
| | 2 | | | |
| | | 3 | | |
| | | | 4 | |
| | | | 5 | |
| | | | | 6 |
| | | | | 7 |

Inbound frames that do not have VLAN tags are tagged with a default service priority of zero, and placed in queue 1 at the output port. Therefore, any inbound frames that do not have priority tags will be placed in queue 1 of the output port. (Note that if the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.) However, if the incoming frame is an IEEE 802.1Q VLAN tagged frame, the IEEE 802.1p User Priority bits will be used.

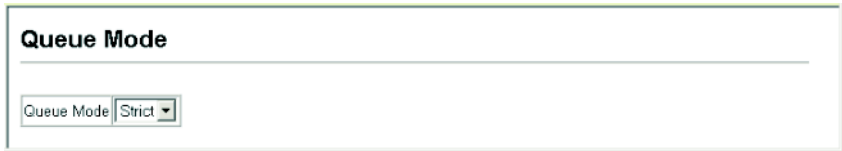
Setting the Queue Mode

You can set the queue mode to strict priority or Weighted Round-Robin (WRR) for the four class of service (CoS) priority queues. The default queue mode is WRR.

Command Attributes

- **WRR** – Weighted Round-Robin shares bandwidth at the egress ports by using scheduling weights of 1, 3, 12 and 48 for queue 0, 1, 2 and 3 respectively.
- **Strict** – Services the egress queues in sequential order, transmitting all traffic in the higher priority queues before servicing lower priority queues.

Web – Click Priority, Queue Mode. Select the required queue mode, click Apply.



Queue Mode

Queue Mode Strict

CLI – This example set the queue mode to use the strict service rule.

```
Console(config)#queue mode strict
Console(config)#
```

3-147

Port Trunk Configuration

You can create multiple links between devices that work as one virtual, aggregate link. A port trunk offers a dramatic increase in bandwidth for network segments where bottlenecks exist, as well as providing a fault-tolerant link between two devices. You can create up to four trunks at a time, with any single trunk containing up to eight ports.

Command Usage

Besides balancing the load across each port in the trunk, the other ports provide redundancy by taking over the load if a port in the trunk fails. However, before making any physical connections between devices, use the Web interface or CLI to specify the trunk on the devices at both ends. When using a port trunk, take note of the following points:

- Finish configuring port trunks before you connect the corresponding network cables between switches to avoid creating a loop.
- The ports at both ends of a connection must be configured as trunk ports.
- When configuring static trunks, you may not be able to link switches of different types, depending on the manufacturer's implementation.
- The ports at both ends of a trunk must be configured in an identical manner, including communication mode (i.e., speed, duplex mode and flow control), VLAN assignments, and CoS settings.
- All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN.
- STP, VLAN, and IGMP settings can only be made for the entire trunk.

Command Attributes

- **Current** – Lists the ports currently configured as members of a static trunk.

- **New** – Selects a predefined port group to add to the specified trunk.

| Group Number | Ports |
|--------------|-------------|
| 1 | 1, 13 |
| 2 | 1-2, 13-14 |
| 3 | 1-4, 13-16 |
| 4 | 5, 17 |
| 5 | 5-6, 17-18 |
| 6 | 5-8, 17-20 |
| 7 | 9, 21 |
| 8 | 9-10, 21-22 |
| 9 | 9-12, 21-24 |
| 10 | 25-26 |

Web – Click Trunk, Trunk Configuration. Enter a trunk ID of 1-4 in the Trunk field, select any of the predefined port groups from the scroll-down list, and click Add. To remove a trunk, type the trunk identifier in the Trunk field, and click Remove.

The screenshot shows a window titled "Trunk Configuration". Inside, there are two main sections: "Member List" and "New".

Member List:

Current:

- Trunk1, Unit1 Port5
- Trunk1, Unit1 Port17

New:

Trunk (1-4): [Text field]

Group: [Dropdown menu showing "1 (1,13)"]

Buttons: <<Add, Remove

CLI – This example creates trunk 1 with ports 5 and 17. Just connect these ports to two static trunk ports on another switch to form a trunk.

| | |
|---|-------|
| Console(config)#interface port-channel 1 | 3-89 |
| Console(config-if)#port-group 4 | 3-152 |
| Console#show interfaces status port-channel 1 | 3-99 |
| Information of Trunk 1 | |
| Basic information: | |
| Port type: 100TX | |
| Mac address: 00-55-FF-FF-DD-E2 | |
| Configuration: | |
| Name: | |
| Port admin: Up | |
| Speed-duplex: Auto | |
| Capabilities: 10half, 10full, 100half, 100full, | |
| Flow control: Disabled | |
| Current status: | |
| Created by: User | |
| Link status: Down | |
| Operation speed-duplex: 10half | |
| Flow control type: None | |
| Member Ports: Eth1/5, Eth1/17, | |
| Console# | |

Configuring SNMP

SNMP (Simple Network Management Protocol) is a communication protocol designed specifically for managing devices or other elements on a network. Equipment commonly managed with SNMP includes switches, routers and host computers. SNMP is typically used to configure these devices for proper operation in a network environment, as well as to monitor them to evaluate performance or detect potential problems.

The switch includes an onboard SNMP agent that continuously monitors the status of its hardware, as well as the traffic passing through its ports. A network management station can access this information using the appropriate software. Access rights to the onboard agent are controlled by community strings. To communicate with the switch, the management station must first

submit a valid community string for authentication. The options for configuring community strings and related trap functions are described in the following sections.

Setting Community Access Strings

You may configure up to five community strings authorized for management access. All community strings used for IP Trap Managers should be listed in this table. For security reasons, you should consider removing the default strings.

Command Attributes

- **SNMP Community Capability** – Indicates that the switch supports up to five community strings.
- **Community String** – A community string that acts like a password and permits access to the SNMP protocol. Default strings: “public” (read-only access), “private” (read/write access)
Range: 1-32 characters, case sensitive
- **Access Mode**
 - **Read-Only** – Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.
 - **Read/Write** – Specifies read-write access. Authorized management stations are able to both retrieve and modify MIB objects.

Web – Click SNMP, SNMP Configuration. Add new community strings as required, select the access rights from the Access Mode drop-down list, then click Add.

SNMP Configuration

SNMP Community:

SNMP Community Capability: 5

Current:

private RW

public RO

<< Add

Remove

New:

Community String

Access Mode

Read-Only

CLI – The following example adds the string “spiderman” with read/write access.

```
Console(config)#snmp-server community spiderman rw
Console(config)#
```

3-54

Specifying Trap Managers and Trap Types

Traps indicating status changes are issued by the switch to specified trap managers. You must specify trap managers so that key events are reported by this switch to your management station (using network management platforms such as HP OpenView). You can specify up to five management stations that will receive authentication failure messages and other trap messages from the switch.

Command Usage

- You can enable or disable authentication messages via the Web interface.
- You can enable or disable authentication messages or link-up-down messages via the CLI.

Command Attributes

- **Trap Manager Capability** – Indicates that the switch supports up to five trap managers.
- **Trap Manager IP Address** – Internet address of the host (the targeted recipient).
- **Trap Manager Community String** – Password-like community string sent with the notification operation. Though you can set this string in the Trap Managers table, we recommend that you define this string in the SNMP Protocol table as well. Range: 1-32 characters, case sensitive.
- **Version** – Indicates if the host is running SNMP version 1 or version 2c.
- **Enable Authentication Traps** – Issues a trap message whenever an invalid community string is submitted during the SNMP access authentication process.
- **Enable Link-up and Link-down traps** – Issues a trap message whenever a port link is established or broken.

Web – Click SNMP, SNMP Configuration. Fill in the IP address and community string for each Trap Manager that will receive these messages, mark Enable Authentication Traps if required, and then click Add.

The screenshot shows a web interface for configuring SNMP trap managers. It has a title 'Trap Managers:' and a sub-header 'Trap Manager Capability: 5'. Under 'Current:', there is a list box containing '(none)'. To its right are two buttons: '<< Add' and 'Remove'. Under 'New:', there is a form with three fields: 'Trap Manager IP address' (a text box), 'Trap Manager Community String' (a text box), and 'Trap Version' (a dropdown menu currently set to '1'). At the bottom, there are two checkboxes: 'Enable Authentication Traps' (checked) and 'Enable Link-up and Link-down Traps' (unchecked).

CLI – This example adds a trap manager and enables authentication traps.

| | |
|--|------|
| Console(config)#snmp-server host 10.1.19.23 batman version 1 | 3-57 |
| Console(config)#snmp-server enable traps authentication | 3-58 |

Multicast Configuration

Multicasting is used to support real-time applications such as video conferencing or streaming audio. A multicast server does not have to establish a separate connection with each client. It merely broadcasts its service to the network, and any hosts that want to receive the multicast register with their local multicast switch/router. Although this approach reduces the network overhead required by a multicast server, the broadcast traffic must be carefully pruned at every multicast switch/router it passes through to ensure that traffic is only passed on the hosts which subscribed to this service.

This switch uses IGMP (Internet Group Management Protocol) to query for any attached hosts that want to receive a specific multicast service. It identifies the ports containing hosts requesting to join the service and sends data out to those ports only. It then propagates the service request up to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service. This procedure is called multicast filtering.

The purpose of IP multicast filtering is to optimize a switched network's performance, so multicast packets will only be forwarded to those ports containing multicast group hosts or multicast routers/switches, instead of flooding traffic to all ports in the subnet (VLAN).

Configuring IGMP Parameters

You can configure the switch to forward multicast traffic intelligently. Based on the IGMP query and report messages, the switch forwards traffic only to the ports that request multicast traffic. This prevents the switch from broadcasting the traffic to all ports and possibly disrupting network performance.

Command Usage

- **IGMP Snooping** – This switch can passively snoop on IGMP Query and Report packets transferred between IP multicast routers/switches and IP multicast host groups to identify the IP multicast group members. It simply monitors the IGMP packets passing through it, picks out the group registration information, and configures multicast filters accordingly.
- **IGMP Query** – A router, or multicast-enabled switch, can periodically ask their hosts if they want to receive multicast traffic. If there is more than one router/switch on the LAN performing IP multicasting, one of these devices is elected “querier” and assumes the role of querying the LAN for group members. It then propagates the service requests on to any

adjacent multicast switch/router to ensure that it will continue to receive the multicast service.

Note: Multicast routers use this information, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet.

Command Attributes

- **IGMP Status** — When enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic. This is also referred to as IGMP Snooping. (Default: Disabled)
- **IGMP Query Count** — Sets the maximum number of queries issued for which there has been no response before the switch takes action to drop a client from the multicast group. (Default: 2, Range: 2 - 10)
- **IGMP Report Delay** — Sets the time (in seconds) between receiving an IGMP Report for an IP multicast address on a port before the switch sends an IGMP Query out of that port and removes the entry from its list. (Default: 10, Range: 5 - 30)
- **Query Timeout** — The time the switch waits after the previous querier stops before it considers the router port (i.e., the interface which had been receiving query packets) to have expired. (Default: 300 seconds, Range: 300 - 500)
- **IGMP Version** — Sets the protocol version for compatibility with other devices on the network. (Default: 2, Range: 1 - 2)

Notes: 1. All systems on the subnet must support the same version.

2. Some attributes are only enabled for IGMPv2, including IGMP Report Delay and IGMP Query Timeout.

Web – Click IGMP, IGMP Configuration. Adjust the IGMP settings as required, and then click Apply. (The default settings are shown below.)

| IGMP Configuration | |
|------------------------------|---------------------------------|
| IGMP Status | <input type="checkbox"/> Enable |
| IGMP Query Count (2-10) | 2 |
| IGMP Report Delay (5-30) | 10 seconds |
| IGMP Query Timeout (300-500) | 300 seconds |
| IGMP Version (1,2) | 2 |

CLI – This example modifies the settings for multicast filtering, and then displays the current status.

```

Console(config)#ip igmp snooping 3-61
Console(config)#ip igmp snooping query-count 10 3-62
Console(config)#ip igmp snooping query-max-response-time 20 3-63
Console(config)#ip igmp snooping router-port-expire-time 300 3-64
Console(config)#ip igmp snooping version 2 3-65
Console(config)#exit
Console#show ip igmp snooping 3-66
  Igmp Snooping Configuration
-----
Service status      : Enabled
Querier status      : Enabled
Query count         : 10
Query interval      : 100 sec
Query max response time : 20 sec
Query time-out      : 300 sec
IGMP snooping version : Version 2
Console#

```

Interfaces Attached to a Multicast Router

Multicast routers use the information obtained from IGMP Query, along with a multicast routing protocol such as DVMRP, to support IP multicasting across the Internet. These routers may be dynamically discovered by the switch or statically assigned to an interface on the switch.

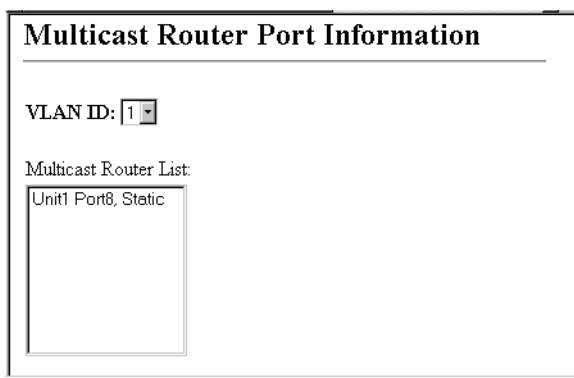
You can use the Multicast Router Port Information page to display the ports on this switch attached to a neighboring multicast router/switch for each VLAN ID.

Displaying Interfaces Attached to a Multicast Router

Command Attributes

- **VLAN ID** – ID of configured VLAN (1-4094).
- **Multicast Router List** – Multicast routers dynamically discovered by this switch or those that are statically assigned to an interface on this switch.

Web – Click IGMP, Multicast Router Port Information. Select the required VLAN ID from the scroll-down list to display the associated multicast routers.



Multicast Router Port Information

VLAN ID: 1

Multicast Router List:

Unit1 Port8, Static

CLI – This example shows that Port 11 has been statically configured as a port attached to a multicast router.

```
Console#show ip igmp snooping mrouter vlan 1
VLAN M'cast Router Port Type
-----
1           Eth 1/11 Static
```

3-165

Specifying Interfaces Attached to a Multicast Router

Depending on your network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/switch connected over the network to an interface (port or trunk) on your switch, you can manually configure that interface to join all the current multicast groups. This can ensure that multicast traffic is passed to all the appropriate interfaces within the switch.

Command Attributes

- **Interface** – Activates the Port or Trunk scroll down list.
- **VLAN ID** – Selects the VLAN to propagate all multicast traffic coming from the attached multicast router/switch.
- **Port** or **Trunk** – Specifies the interface attached to a multicast router.

Web – Click IGMP, Static Multicast Router Port Configuration. Specify the interfaces attached to a multicast router, indicate the VLAN which will forward all the corresponding multicast traffic, and then click Add. After you have completed adding interfaces to the list, click Apply.

Static Multicast Router Port Configuration

Current:

Vlan1, Unit1 Port8

New:

| | |
|-----------|------|
| Interface | Port |
| VLAN ID | 1 |
| Port | 1 |
| Trunk | |

<<Add

Remove

CLI – This example configures port 11 as a multicast router port within VLAN 1.

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/11 3-164
Console(config)#exit
Console#show ip igmp snooping mrouter vlan 1 3-165
VLAN M'cast Router Port Type
-----
1 Eth 1/11 Static
```

Displaying Port Members of Multicast Services

You can display the port members associated with a specified VLAN and multicast IP address.

Command Attribute

- **VLAN ID** – Selects the VLAN in which to display port members.
- **Multicast IP Address** – The IP address for a specific multicast service
- **Multicast Group Port List** – Ports propagating a multicast service; i.e., ports that belong to the indicated VLAN group.

Web – Click IGMP, IP Multicast Registration Table. Select the VLAN ID and multicast IP address. The switch will display all the ports that are propagating this multicast service.

IP Multicast Registration Table

VLAN ID:

Multicast IP Address:

Multicast Group Port List:

| Unit1 Port7, User |
|-------------------|
| |

CLI – This example displays all the known multicast services supported on VLAN 1, along with the ports propagating the corresponding services. The type field shows if this entry was learned dynamically or was statically configured.

```

Console#show mac-address-table multicast vlan 1
VLAN M'cast IP addr. Member ports Type
-----
1      224.0.0.12      Eth1/12      USER
1      224.1.2.3       Eth1/12      IGMP
Console#

```

3-158

Adding Multicast Addresses to VLANs

Multicast filtering can be dynamically configured using IGMP Snooping and IGMP Query messages as described in “Configuring IGMP Parameters” on page 2-87. For certain application that require tighter control, you may need to statically configure a multicast service on the switch. First add all the ports attached to participating hosts to a common VLAN, and then assign the multicast service to that VLAN group.

Command Usage

- Static multicast addresses are never aged out.
- When a multicast address is assigned to specific VLAN, the corresponding traffic can only be forwarded to ports within that VLAN.

Command Attribute

- **Interface** – Activates the Port or Trunk scroll down list.
- **VLAN ID** – Selects the VLAN to propagate all multicast traffic coming from the attached multicast router/switch.
- **Multicast IP** – The IP address for a specific multicast service
- **Port** or **Trunk** – Specifies the interface attached to a multicast router.

Web – Click IGMP, IGMP Member Port Table. Specify the interface attached to a multicast service (via an IGMP-enabled switch or multicast router), indicate the VLAN that will propagate the multicast service, specify the multicast IP address, and then click Add. After you have completed adding ports to the member list, click Apply.

IGMP Member Port Table

IGMP Member Port List:

| |
|-------------------------------------|
| VLAN 1, 224.128.0.9, Unit 1, Port 7 |
|-------------------------------------|

<<Add

Remove

New Static IGMP Member Port:

| | |
|--------------|--------------------------|
| Interface | Port ▾ |
| VLAN ID | 1 ▾ |
| Multicast IP | |
| Port | 1 ▾ |
| Trunk | <input type="checkbox"/> |

CLI – This example assigns a multicast address to VLAN 1, and then displays all the known multicast services supported on VLAN 1.

```

Console(config)#ip igmp snooping vlan 1 static 224.0.0.12
ethernet 1/12
Console(config)#exit
Console#show mac-address-table multicast vlan 1
VLAN M'cast IP addr. Member ports Type
-----
1      224.0.0.12      Eth1/12  USER
1      224.1.1.2.3      Eth1/12  IGMP
Console#
  
```

3-156
3-158

Showing Port Statistics

You can display standard statistics on network traffic from the Interfaces Group and Ethernet-like MIBs, as well as a detailed breakdown of traffic based on the RMOM MIB. Interfaces and Ethernet-like statistics display errors on the traffic passing through each port. This information can be used to identify potential problems with the switch (such as a faulty port or unusually heavy loading). RMON statistics provide access to a broad range of statistics, including a total count of different frame types and sizes passing through each port. All values displayed have been accumulated since the last system reboot, and are shown as counts per second. Statistics are refreshed every 60 seconds by default.

Note: RMON groups 2, 3 and 9 can only be accessed using SNMP management software such as EliteView.

Web – Click Statistics, Port Statistics. Select the required interface, and click Query. You can also use the Refresh button at the bottom of the page to update the screen.

Port Statistics

Interface
Port 1
Trunk 1

Query

Interface Statistics:

| | | | |
|----------------------------|--------|----------------------------|---------|
| Received Octets | 140335 | Received Unicast Packets | 1335 |
| Received Multicast Packets | 0 | Received Broadcast Packets | 17 |
| Received Discarded Packets | 0 | Received Unknown Packets | 0 |
| Received Errors | 0 | Transmit Octets | 1695197 |
| Transmit Unicast Packets | 1624 | Transmit Multicast Packets | 923 |
| Transmit Broadcast Packets | 2 | Transmit Discarded Packets | 0 |
| Transmit Errors | 0 | | |

Etherlike Statistics:

| | | | |
|---------------------------|---|------------------------------|---|
| Alignment Errors | 0 | Late Collisions | 0 |
| FCS Errors | 0 | Excessive Collisions | 0 |
| Single Collision Frames | 0 | Internal MAC Transmit Errors | 0 |
| Multiple Collision Frames | 0 | Carrier Sense Errors | 0 |
| SQE Test Errors | 0 | Frames Too Long | 0 |
| Deferred Transmissions | 0 | Internal MAC Receive Errors | 0 |

RMON Statistics:

| | | | |
|----------------------|--------|------------------------|------|
| Drop Events | 0 | Jabbers | 0 |
| Received Bytes | 147563 | Collisions | 0 |
| Received Frames | 0 | 64 Bytes Frames | 1120 |
| Broadcast Frames | 17 | 65-127 Bytes Frames | 157 |
| Multicast Frames | 0 | 128-255 Bytes Frames | 5 |
| CRC/Alignment Errors | 0 | 256-511 Bytes Frames | 138 |
| Undersize Frames | 0 | 512-1023 Bytes Frames | 6 |
| Oversize Frames | 0 | 1024-1518 Bytes Frames | 0 |
| Fragments | 0 | | |

CLI – This example shows statistics for port 1.

```
Console#show interfaces counters ethernet 1/13 3-100
Ethernet 1/ 1
Iftable stats:
  Octets input: 163138, Octets output: 2056071
  Unicast input: 1564, Unicast output: 1918
  Discard input: 0, Discard output: 0
  Error input: 0, Error output: 0
  Unknown protos input: 0, QLen output: 0
Extended iftable stats:
  Multi-cast input: 0, Multi-cast output: 1118
  Broadcast input: 18, Broadcast output: 2
Ether-like stats:
  Alignment errors: 0, FCS errors: 0
  Single Collision frames: 0, Multiple collision frames: 0
  SQE Test errors: 0, Deferred transmissions: 0
  Late collisions: 0, Excessive collisions: 0
  Internal mac transmit errors: 0, Internal mac receive errors: 0
  Frame too longs: 0, Carrier sense errors: 0
  Symbol errors: 0
RMON stats:
  Drop events: 0, Octets: 163138, Packets: 1582
  Broadcast pkts: 18, Multi-cast pkts: 0
  Undersize pkts: 0, Oversize pkts: 0
  Fragments: 0, Jabbers: 0
  CRC align errors: 0, Collisions: 0
  Packet size <= 64 octets: 1249, Packet size 65 to 127 octets: 170
  Packet size 128 to 255 octets: 6, Packet size 256 to 511 octets: 151
  Packet size 512 to 1023 octets: 6, Packet size 1024 to 1518 octets: 0
Console#
```

Rate Limit Configuration

This function allows the network manager to control the maximum rate for traffic transmitted or received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the network. Traffic that falls within the rate limit is transmitted, while packets that exceed the acceptable amount of traffic are dropped.

Rate limiting can be applied to individual ports or trunks. When an interface is configured with this feature, the traffic rate will be monitored by the hardware to verify conformity. Non-conforming traffic is dropped, conforming traffic is forwarded without any changes.

Command Attribute

- **Port/Trunk** – The switch interface.
- **Rate Limit Status** – Enables or disables the rate limit.
- **Rate Limit (Percent)** – Sets the rate limit to predefined percentage of bandwidth.

| Option | Percentage (based on port type) | | |
|---------------|--|-----------------|------------------|
| | 10 Mbps | 100 Mbps | 1000 Mbps |
| 3 | 312K | 3.12M | 31.2M |
| 6 | 625K | 6.25M | 62.5M |
| 9 | 938K | 9.38M | 93.8M |
| 12 | 1.25M | 12.5M | 125M |
| 20 | 2M | 20M | 200M |
| 40 | 4M | 40M | 400M |
| 60 | 6M | 60M | 600M |
| 80 | 8M | 80M | 800M |

Web - Click Rate Limit, Input/Output Rate Limit Port/Trunk Configuration. Enable the Rate Limit Status for the required interfaces, set the Rate Limit to one of the options shown in the preceding table, and click Apply.

Input Rate Limit Port Configuration

| Port | Input Rate Limit Status | Input Rate Limit(percent) | Trunk |
|------|-------------------------|---------------------------|-------|
| 1 | Disabled | 3 | |
| 2 | Disabled | 0 | |
| 3 | Enabled | 3 | |
| 4 | Enabled | 6 | |
| 5 | Disabled | 0 | |

CLI - This example sets the rate limit for input and output traffic passing through port 3 to approximately 3% (i.e., 3.12 Mbps for a 100 Mbps link), and the rate limit for traffic crossing port 4 to 6% (i.e., 6.25 Mbps for a 100 Mbps link).

Console(config)#interface ethernet 1/33-89
Console(config-if)#rate-limit input percent 33-105
Console(config-if)#rate-limit output percent 3
Console(config-if)#exit
Console(config)#interface ethernet 1/4
Console(config-if)#rate-limit input percent 63-105
Console(config-if)#rate-limit output percent 6
Console(config-if)#

Configuring 802.1x Port Authentication

Network switches can provide open and easy access to network resources by simply attaching a client PC. Although this automatic configuration and access is a desirable feature, it also allows unauthorized personnel to easily intrude and possibly gain access to sensitive network data.

The IEEE 802.1x (dot1x) standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first enter a user ID and password for authentication. Access to all switch ports in a network can be centrally controlled from a server, which means that authorized users can use a single user ID and password for authentication from any point within the network.

This switch uses the Extensible Authentication Protocol over LAN (EAPOL) with MD5 authentication to exchange authentication protocol messages with the client, and a remote login authentication server (i.e., RADIUS) to verify user identity and access rights. When a client (i.e., Supplicant) connects to a switch port, the switch (i.e., Authenticator) responds with an identity request. The client provides its identity to the switch, which it forwards to the authentication server. The authentication server verifies the client identity and sends this information back to the switch. The switch then issues an MD5 access challenge to the client, and the client returns an MD5 response to the switch based on its user ID and password. If authentication is successful, the switch allows the client to access the network. Otherwise, network access is denied and the port remains blocked.

The operation of dot1x on the switch requires the following:

- The switch must have an IP address assigned.
- RADIUS authentication must be enabled on the switch and the IP address of the RADIUS server specified.
- Each switch port that will be used must be set to dot1x “Auto” mode.
- Each client that needs to be authenticated must have dot1x client software installed and properly configured.

Displaying 802.1x Global Settings

The dot1x protocol includes global parameters that control the client authentication process that runs between the client and the switch (i.e., authenticator), as well as the client identity lookup process that runs between the switch and authentication server. These parameters are described in this section.

Command Attributes

- **dot1X Re-authentication** – Indicates if switch ports require a client to be re-authenticated after a certain period of time.
- **dot1X Max Request Count** – The maximum number of times the switch port will retransmit an EAP request packet to the client before it times out the authentication session.
- **Timeout for Quiet Period** – Indicates the time that a switch port waits after the Max Request Count has been exceeded before attempting to acquire a new client.
- **Timeout for Re-authentication Period** – Indicates the time period after which a connected client must be re-authenticated.
- **Timeout for TX Period** – The time period during an authentication session that the switch waits before re-transmitting an EAP packet.
- **Supplicant timeout** – The time the switch waits for a client response to an EAP request.
- **Server timeout** – The time the switch waits for a response from the RADIUS server to an authentication request.
- **Re-authentication Max Count** – The number of times the switch will attempt to re-authenticate a connected client.

Web – Click dot1x, dot1X Information.

dot1X Information

| | |
|--------------------------------------|--------------|
| dot1X Re-authentication | Disabled |
| dot1X Max Request Count | 2 |
| Timeout for Quiet Period | 60 seconds |
| Timeout for Re-authentication Period | 3600 seconds |
| Timeout for Tx Period | 30 seconds |
| Supplicant timeout | 30 seconds |
| Server timeout | 30 seconds |
| Re-authentication Max Count | 2 |

CLI -This example shows the default protocol settings for dot1x.

3-51

```

Console#show dot1x
Global 802.1X Parameters
reauth-enabled: n/a
reauth-period: 3600
quiet-period: 60
tx-period: 30
supp-timeout: 30
server-timeout: 30
reauth-max: 2
max-reg: 2

802.1X Port Summary
  Port Name      Status      Mode      Authorized
    1           disabled   ForceAuthorized   n/a
    2           disabled   ForceAuthorized   yes
    3           disabled   ForceAuthorized   n/a
    4           disabled   ForceAuthorized   n/a
    .....
   23           disabled   ForceAuthorized   n/a
   24           disabled   ForceAuthorized   n/a
Console#

```

Configuring 802.1x Global Settings

The dot1x protocol includes global parameters that control the client authentication process that runs between the client and the switch (i.e., authenticator), as well as the client

identity lookup process that runs between the switch and authentication server. The configuration options for parameters are described in this section.

Command Attributes

- **dot1X Re-authentication** – Sets the client to be re-authenticated after the interval specified by the Timeout for Re-authentication Period. Re-authentication can be used to detect if a new device is plugged into a switch port. (Default: Disabled)
- **dot1X Max Request Count** – Sets the maximum number of times the switch port will retransmit an EAP request packet to the client before it times out the authentication session. (Range: 1-10; Default 2)
- **Timeout for Quiet Period** – Sets the time that a switch port waits after the dot1X Max Request Count has been exceeded before attempting to acquire a new client. (Range: 1-65535 seconds; Default: 60 seconds)
- **Timeout for Re-authentication Period** – Sets the time period after which a connected client must be re-authenticated. (Range: 1-65535 seconds; Default: 3600 seconds)
- **Timeout for TX Period** – Sets the time period during an authentication session that the switch waits before re-transmitting an EAP packet. (Range: 1-65535; Default: 30 seconds)
- **authentication dot1x*** – Sets the default authentication server type. Note the specified authentication server type must be enabled and properly configured for dot1x to function properly. (Options: radius)

* CLI only.

Web – Select dot1x, dot1X Configuration. Enable dot1x globally for the switch, modify any of the parameters required, and then click Apply.

dot1X Configuration

| | |
|--|--|
| dot1X Re-authentication | <input type="checkbox"/> Enable |
| dot1X Max Request Count (1-10) | <input style="width: 50px;" type="text" value="2"/> |
| Timeout for Quiet Period (0-65535) | <input style="width: 50px;" type="text" value="60"/> seconds |
| Timeout for Re-authentication Period (0-65535) | <input style="width: 50px;" type="text" value="3600"/> seconds |
| Timeout for Tx Period (1-65535) | <input style="width: 50px;" type="text" value="30"/> seconds |

CLI – This example enables re-authentication and sets all of the global parameters for dot1x.

| | |
|---|------|
| Console(config)#dot1x max-req 5 | 3-46 |
| Console(config)#dot1x re-authentication | 3-48 |
| Console(config)#dot1x timeout quiet-period 40 | 3-49 |
| Console(config)#dot1x timeout re-auth 5 | 3-49 |
| Console(config)#dot1x timeout tx-period 40 | 3-50 |
| Console(config)#authentication dot1x default radius | 3-45 |
| Console(config)# | |

Configuring a Port for Authorization

When dot1x is enabled, you need to specify the dot1x authentication mode configured for each port.

Command Attributes

- **Status** – Indicates if authentication is enabled or disabled on the port.

- **Mode** – Sets the authentication mode to one of the following options:
 - **Force-Authorized** – Configures the port to grant access to all clients, either dot1x-aware or otherwise.
 - **Force-Unauthorized** – Configures the port to deny access to all clients, either dot1x-aware or otherwise.
 - **Auto** – Requires a dot1x-aware connected client to be authorized by the RADIUS server. Clients that are not dot1x-aware will be denied access.
- **Authorized** –
 - **Yes** – Connected client is authorized.
 - **No** – Connected client is not authorized.
 - *Blank* – Displays nothing when dot1x is disabled on a port.
- **Supplicant** – Indicates the MAC address of a connected client.
- **Trunk** – Indicates if the port is configured as a trunk port.

Web – Click dot1x, dot1X Port Configuration then select the Mode from the drop- down list.

| dot1X Port Configuration | | | | | |
|--------------------------|----------|--------------------|------------|-------------------|-------|
| Port | Status | Mode | Authorized | Supplicant | Trunk |
| 1 | Disabled | Force-Authorized ▼ | | 00-00-00-00-00-00 | |
| 2 | Disabled | Force-Authorized ▼ | | 00-00-00-00-00-00 | |
| 3 | Disabled | Force-Authorized ▼ | | 00-00-00-00-00-00 | |
| 4 | Disabled | Force-Authorized ▼ | Yes | 00-00-00-00-00-00 | |
| 5 | Disabled | Force-Authorized ▼ | | 00-00-00-00-00-00 | |
| 6 | Disabled | Force-Authorized ▼ | | 00-00-00-00-00-00 | |

CLI – This example sets the authentication mode to enable dot1x on port 2.

```
Console(config)#interface ethernet 1/2
Console(config-if)#dot1x port-control auto
Console(config-if)#
```

3-47

Displaying 802.1x Statistics

This switch can display statistics for dot1x protocol exchanges for any port.

Statistical Values

| Parameter | Description |
|------------------|--|
| Rx EXPOL Start | The number of EAPOL Start frames that have been received by this Authenticator. |
| Rx EAPOL Logoff | The number of EAPOL Logoff frames that have been received by this Authenticator. |
| Rx EAPOL Invalid | The number of EAPOL frames that have been received by this Authenticator in which the frame type is not recognized. |
| Rx EAPOL Total | The number of valid EAPOL frames of any type that have been received by this Authenticator. |
| Rx EAP Resp/Id | The number of EAP Resp/Id frames that have been received by this Authenticator. |
| Rx EAP Resp/Oth | The number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Authenticator. |
| Rx EAP LenError | The number of EAPOL frames that have been received by this Authenticator in which the Packet Body Length field is invalid. |
| Rx Last EAPOLVer | The protocol version number carried in the most recently received EAPOL frame. |
| Rx Last EAPOLSrc | The source MAC address carried in the most recently received EAPOL frame. |

| Parameter | Description |
|----------------|--|
| Tx EAPOL Total | The number of EAPOL frames of any type that have been transmitted by this Authenticator. |
| Tx EAP Req/Id | The number of EAP Req/Id frames that have been transmitted by this Authenticator. |
| Tx EAP Req/Oth | The number of EAP Request frames (other than Rq/Id frames) that have been transmitted by this Authenticator. |

Web – Select dot1x followed by dot1X statistics. Select the required port and then click Query. Click Refresh to update statistics.

dot1X Statistics

Port1

Query

| | | | |
|------------------|--|------------------|--|
| Rx EXPOL Start | | Rx EAP LenError | |
| Rx EAPOL Logoff | | Rx Last EAPOLVer | |
| Rx EAPOL Invalid | | Rx Last EAPOLSrc | |
| Rx EAPOL Total | | Tx EAPOL Total | |
| Rx EAP Resp/Id | | Tx EAP Req/Id | |
| Rx EAP Resp/Oth | | Tx EAP Req/Oth | |

Refresh

CLI – This example displays the dot1x statistics for port 1.

```

Console#show dot1x statistics

Eth 1/1
Rx: EXPOL      EAPOL      EAPOL      EAPOL      EAP      EAP      EAP
    Start      Logoff    Invalid    Total      Resp/Id   Resp/Oth LenError
        0          0          0          0          0          0          0

    Last      Last
EAPOLVer      EAPOLSrc
    0          00-00-00-00-00-00

Tx: EAPOL      EAP      EAP
    Total      Req/Id   Req/Oth
        0          0          0
Console#

```


CHAPTER 3

COMMAND LINE INTERFACE

This chapter describes how to use the Command Line Interface (CLI).

Using the Command Line Interface

Accessing the CLI

When accessing the management interface for the switch over a direct connection to the server's console port, or via a Telnet connection, the switch can be managed by entering command keywords and parameters at the prompt. Using the switch's command-line interface (CLI) is very similar to entering commands on a UNIX system.

Console Connection

To access the switch through the console port, perform these steps:

1. At the console prompt, enter the user name and password. (The default user names are "admin" and "guest" with corresponding passwords of "admin" and "guest.") When the administrator user name and password is entered, the CLI displays the "Console#" prompt and enters privileged access mode (i.e., Privileged Exec). But when the guest user name and password is entered, the CLI displays the "Console>" prompt and enters normal access mode (i.e., Normal Exec).

2. Enter the necessary commands to complete your desired tasks.
3. When finished, exit the session with the “quit” or “exit” command.

After connecting to the system through the console port, the login screen displays:

```
User Access Verification

Username: admin
Password:

      CLI session with the TigerSwitch 10/100 -
      6724L2 Managed 24+2 Standalone Switch is opened.
      To end the CLI session, enter [Exit].

Console#
```

Telnet Connection

Telnet operates over the IP transport protocol. In this environment, your management station and any network device you want to manage over the network must have a valid IP address. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Each address consists of a network portion and host portion. For example, the IP address assigned to this switch, 10.1.0.1, consists of a network portion (10.1.0) and a host portion (1).

Note: The IP address for this switch is unassigned by default.

To access the switch through a Telnet session, you must first set the IP address for the switch, and set the default gateway if you are managing the switch from a different IP subnet. For example,

```
Console(config)#interface vlan 1
Console(config-if)#ip address 10.1.0.1 255.255.255.0
Console(config-if)#exit
Console(config)#ip default-gateway 10.1.0.254
```


If your corporate network is connected to another network outside your office or to the Internet, you need to apply for a registered IP address. However, if you are attached to an isolated network, then you can use any IP address that matches the network segment to which you are attached.

After you configure the switch with an IP address, you can open a Telnet session by performing these steps.

1. From the remote host, enter the Telnet command and the IP address of the device you want to access.
2. At the prompt, enter the user name and system password. The CLI will display the “Vty-0#” prompt for the administrator to show that you are using privileged access mode (i.e., Privileged Exec), or “Vty-0>” for the guest to show that you are using normal access mode (i.e., Normal Exec).
3. Enter the necessary commands to complete your desired tasks.
4. When finished, exit the session with the “quit” or “exit” command.

After entering the Telnet command, the login screen displays:

```
Username: admin
Password:

      CLI session with the ES-3526N-ZZ Intelligent Switch is opened.
      To end the CLI session, enter [Exit].

Vty-0#
```

Note: You can open up to four sessions to the device via Telnet

Entering Commands

This section describes how to enter CLI commands.

Keywords and Arguments

A CLI command is a series of keywords and arguments. Keywords identify a command, and arguments specify configuration parameters. For example, in the command “show interfaces status ethernet 1/5,” **show interfaces** and **status** are keywords, **ethernet** is an argument that specifies the interface type, and **1/5** specifies the unit/port.

You can enter commands as follows:

- To enter a simple command, enter the command keyword.
- To enter multiple commands, enter each command in the required order. For example, to enable Privileged Exec command mode, and display the startup configuration, enter:

```
Console>enable  
Console#show startup-config
```

- To enter commands that require parameters, enter the required parameters after the command keyword. For example, to set a password for the administrator, enter:

```
Console(config)#username admin password 0 smith
```

Minimum Abbreviation

The CLI will accept a minimum number of characters that uniquely identify a command. For example, the command “configure” can be entered as **config**. If an entry is ambiguous, the system will prompt for further input.

Command Completion

If you terminate input with a Tab key, the CLI will print the remaining characters of a partial keyword up to the point of ambiguity. In the “logging history” example, typing **log** followed by a tab will result in printing the command up to “**logging**.”

Getting Help on Commands

You can display a brief description of the help system by entering the **help** command. You can also display command syntax by using the “?” character to list keywords or parameters.

Showing Commands

If you enter a “?” at the command prompt, the system will display the first level of keywords for the current command class (Normal Exec or Privileged Exec) or configuration class (Global, Interface, Line, or VLAN Database). You can also display a list of valid keywords for a specific command. For example, the command “**show ?**” displays a list of possible show commands:

```
Console#show ?
  bridge-ext      Bridge extend information
  garp            Garp property
  gvrp            Show GVRP information of interface
  history         Information of history
  interfaces      Information of interfaces
  ip             Ip
  line           TTY line information
  mac-address-table Set configuration of the address table
  port           Characteristics of the port
  queue          Information of priority queue
  radius-server  RADIUS server information
  running-config The system configuration of running
  snmp           SNMP statistics
  spanning-tree  Specify spanning-tree
  startup-config The system configuration of starting up
  system        Information of system
  users         Display information about terminal lines
  version       System hardware and software status
  vlan         Switch VLAN Virtual Interface
Console#show
```

The command “**show interfaces ?**” will display the following information:

```
Console>show interfaces ?
  counters      Information of interfaces counters
  status        Information of interfaces status
  switchport    Information of interfaces switchport
```

Partial Keyword Lookup

If you terminate a partial keyword with a question mark, alternatives that match the initial letters are provided. (Remember not to leave a space between the command and question mark.) For example “**s?**” shows all the keywords starting with “s.”

```
Console#show s?
  snmp  spanning-tree  startup-config  system
Console#show s
```

Negating the Effect of Commands

For many configuration commands you can enter the prefix keyword “**no**” to cancel the effect of a command or reset the configuration to the default value. For example, the **logging** command will log system messages to a host server. To disable logging, specify the **no logging** command. This guide describes the negation effect for all applicable commands.

Using Command History

The CLI maintains a history of commands that have been entered. You can scroll back through the history of commands by pressing the up arrow key. Any command displayed in the history list can be executed again, or first modified and then executed.

Using the **show history** command displays a longer list of recently executed commands.

Understanding Command Modes

The command set is divided into Exec and Configuration classes. Exec commands generally display information on system status or clear statistical counters. Configuration commands, on the other hand, modify interface parameters or enable certain switching functions. These classes are further divided into different modes. Available commands depend on the selected mode. You can always enter a question mark “?” at the prompt to display a list of the commands available for the current mode. The command classes and associated modes are displayed in the following table:

| Class | Mode |
|----------------|------------|
| Exec | Normal |
| | Privileged |
| Configuration* | Global |
| | Interface |
| | Line |
| | VLAN |

* You must be in Privileged Exec mode to access any of the configuration modes.

Exec Commands

When you open a new console session on the switch with the user name and password “guest,” the system enters the Normal Exec command mode (or guest mode), displaying the “Console>” command prompt. Only a limited number of the commands are available in this mode. You can access all commands only from the Privileged Exec command mode (or administrator mode). To access Privilege Exec mode, open a new console session with the user name and password “admin.” The system will now displays the “Console#” command prompt. You can also enter Privileged Exec mode from within Normal Exec mode, by entering the

enable command, followed by the privileged level password “super” (page 3-29).

To enter Privileged Exec mode, enter the following commands and passwords:

```
Username: admin
Password: [admin login password]

      CLI session with the TigerSwitch 10/100 - 6724L2 Managed 24+2
      Standalone Switch is opened.
      To end the CLI session, enter [Exit].

Console#
```

```
Username: guest
Password: [system login password]

      CLI session with the TigerSwitch 10/100 - 6724L2 Managed 24+2
      Standalone Switch is opened.
      To end the CLI session, enter [Exit].

Console#enable
Password: [privileged level password if so configured]
Console#
```

Configuration Commands

Configuration commands are privileged level commands used to modify switch settings. These commands modify the running configuration only and are not saved when the switch is rebooted. To store the running configuration in nonvolatile storage, use the **copy running-config startup-config** command.

The configuration commands are organized into four different modes:

- Global Configuration - These commands modify the system level configuration, and include commands such as **hostname** and **snmp-server community**.

- Interface Configuration - These commands modify the port configuration such as **speed-duplex** and **negotiation**.
- Line Configuration - These commands modify the console port and Telnet configuration, and include command such as **parity** and **databits**.
- VLAN Configuration - Includes the command to create VLAN groups.

To enter the Global Configuration mode, enter the command **configure** in Privileged Exec mode. The system prompt will change to “Console(config)#” which gives you access privilege to all Global Configuration commands.

```
Console#configure
Console(config)#
```

To enter the other modes, at the configuration prompt type one of the following commands. Use the **exit** or **end** command to return to the Privileged Exec mode.

| Mode | Command | Prompt | Page |
|-----------|---|-----------------------|-------|
| Interface | interface {ethernet <i>port</i> port-channel <i>id</i> vlan <i>id</i> } | Console(config-if)# | 3-86 |
| Line | line {console vty} | Console(config-line)# | 3-61 |
| VLAN | vlan database | Console(config-vlan)# | 3-121 |

For example, you can use the following commands to enter interface configuration mode, and then return to Privileged Exec mode

```
Console(config)#interface ethernet 1/5
.
.
.
Console(config-if)#exit
Console(config)#
```

Command Line Processing

Commands are not case sensitive. You can abbreviate commands and parameters as long as they contain enough letters to differentiate them from any other currently available commands or parameters. You can use the Tab key to complete partial commands, or enter a partial command followed by the “?” character to display a list of possible matches. You can also use the following editing keystrokes for command-line processing:

| Keystroke | Function |
|--------------------------------|---|
| Ctrl-A | Shifts cursor to start of command line. |
| Ctrl-B | Shifts cursor to the left one character. |
| Ctrl-E | Shifts cursor to end of command line. |
| Ctrl-F | Shifts cursor to the right one character. |
| Ctrl-P | Shows the last command. |
| Ctrl-U | Deletes the entire line. |
| Ctrl-W | Deletes the last word typed. |
| Delete key or backspace key | Erases a mistake when entering a command. |

Command Groups

The system commands can be broken down into the functional groups shown below.

| Command Group | Description | Page |
|-------------------|--|------|
| General | Basic commands for entering privileged access mode, restarting the system, or quitting the CLI | 3-13 |
| Flash/File | Manages code image or switch configuration files | 3-19 |
| System Management | Controls system logs, system passwords, user name, browser management options, and a variety of other system information | 3-26 |

| Command Group | Description | Page |
|---------------------------|---|-------------|
| RADIUS Client | Configures RADIUS client-server authentication for logon access | 3-38 |
| Port Authentication | Configures IEEE 802.1x port access control | 3-44 |
| SNMP | Activates authentication failure traps; configures community access strings, and trap managers | 3-54 |
| IGMP Snooping | Configures IGMP multicast filtering, querier eligibility, query parameters, and specifies ports attached to a multicast router | 3-61 |
| Line | Sets communication parameters for the serial port and Telnet, including baud rate and console time-out | 3-68 |
| IP | Configures the IP address and gateway for management access, displays the default gateway, or pings a specified device | 3-79 |
| HOL Blocking Prevention | Enables head-of-line (HOL) Blocking Prevention on the switch | 3-86 |
| Interface | Configures the connection parameters for all Ethernet ports, aggregated links, and VLANs | 3-88 |
| Rate Limiting | Sets the maximum rate for traffic transmitted or received on an interface | 3-104 |
| Address Table | Configures the address table for filtering specified addresses, displaying current entries, clearing the table, or setting the aging time | 3-106 |
| Spanning Tree | Configures Spanning Tree settings for the switch | 3-111 |
| VLAN | Configures VLAN settings, defines port membership for VLAN groups | 3-121 |
| PVLAN | Enables or configures private VLANs | 3-132 |
| GVRP and Bridge Extension | Configures GVRP settings that permit automatic VLAN learning; shows the configuration for bridge extension MIB | 3-140 |
| Priority | Sets port priority for untagged frames, also sets the service weight for each priority queue based on strict priority or Weighted Round Robin | 3-146 |

| Command Group | Description | Page |
|----------------------|---|-------------|
| Mirror Port | Mirrors data to another port for analysis without affecting the data passing through or the performance of the monitored port | 3-148 |
| Port Trunking | Statically groups multiple ports into a single logical trunk | 3-150 |

Note: Note that the access mode shown in the following tables is indicated by these abbreviations:

NE (Normal Exec)

PE (Privileged Exec)

GC (Global Configuration)

IC (Interface Configuration)

LC (Line Configuration)

VC (VLAN Database Configuration)

General Commands

| Command | Function | Mode | Page |
|--------------|--|----------------|------|
| enable | Activates privileged mode | NE | 3-13 |
| disable | Returns to normal mode from privileged mode | PE | 3-14 |
| configure | Activates global configuration mode | PE | 3-15 |
| show history | Shows the command history buffer | NE, PE | 3-16 |
| reload | Restarts the system | PE | 3-17 |
| end | Returns to Privileged Exec mode | GC, IC, LC, VC | 3-17 |
| exit | Returns to the previous configuration mode, or exits the CLI | any | 3-18 |
| quit | Exits a CLI session | NE, PE | 3-19 |
| help | Shows how to use help | any | NA |
| ? | Shows options for command completion (context sensitive) | any | NA |

enable

Use this command to activate Privileged Exec mode. In privileged mode, additional commands are available, and certain commands display additional information. See “Understanding Command Modes” on page 3-7.

Syntax

enable [*level*]

level - Privilege level to log into the device.

The device has two predefined privilege levels:

0: Normal Exec, 15: Privileged Exec. Enter level 15 to access Privileged Exec mode.

Default Setting

Level 15

Command Mode

Normal Exec

Command Usage

- “super” is the default password required to change the command mode from Normal Exec to Privileged Exec. (To set this password, see the **enable password** command on page 3-29.)
- The “#” character is appended to the end of the prompt to indicate that the system is in privileged access mode.

Example

```
Console#enable
Password: [privileged level password]
Console#
```

Related Commands

enable password (3-29)

disable

Use this command to return to Normal Exec mode from privileged mode. In normal access mode, you can only display basic information on the switch's configuration or Ethernet statistics. To gain access to all commands, you must use the privileged mode. See “Understanding Command Modes” on page 3-7.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

The “>” character is appended to the end of the prompt to indicate that the system is in normal access mode.

Example

```
Console#disable  
Console>
```

Related Commands

enable (3-13)

configure

Use this command to activate Global Configuration mode. You must enter this mode to modify any settings on the switch. You must also enter Global Configuration mode prior to enabling some of the other configuration modes, including Interface Configuration, Line Configuration, and VLAN Database Configuration. See “Understanding Command Modes” on page 3-7.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#configure  
Console(config)#
```

Related Commands

end (3-17)

show history

Use this command to show the contents of the command history buffer.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

The history buffer size is fixed at 10 Execution commands and 10 Configuration commands.

Example

In this example, the show history command lists the contents of the command history buffer:

```
Console#show history
Execution command history:
 2 config
 1 show history

Configuration command history:
 4 interface vlan 1
 3 exit
 2 interface vlan 1
 1 end

Console#
```

The **!** command repeats commands from the Execution command history buffer when you are in Normal Exec or Privileged Exec Mode, and commands from the Configuration command history buffer when you are in any of the configuration modes. In this

example, the **!2** command repeats the second command in the Execution history buffer (**config**).

```
Console#!2
Console#config
Console(config)#
```

reload

Use this command to restart the system.

Note: When the system is restarted, it will always run the Power-On Self-Test. It will also retain all configuration information stored in non-volatile memory by the **copy running-config startup-config** command.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

This command resets the entire system.

Example

This example shows how to reset the switch:

```
Console#reload
System will be restarted, continue <y/n>? y
```

end

Use this command to return to Privileged Exec mode.

Default Setting

None

Command Mode

Global Configuration, Interface Configuration, Line Configuration, VLAN Database Configuration

Example

This example shows how to return to the Privileged Exec mode from the Interface Configuration mode:

```
Console(config-if)#end
Console#
```

exit

Use this command to return to the previous configuration mode or exit the configuration program.

Default Setting

None

Command Mode

Any

Example

This example shows how to return to the Privileged Exec mode from the Global Configuration mode, and then quit the CLI session:

```
Console(config)#exit
Console#exit

Press ENTER to start session

User Access Verification

Username:
```


quit

Use this command to exit the configuration program.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

The quit and exit commands can both exit the configuration program.

Example

This example shows how to quit a CLI session:

```
Console#quit  
  
Press ENTER to start session  
  
User Access Verification  
  
Username:
```

Flash/File Commands

These commands are used to manage the system code or configuration files.

| Command | Function | Mode | Page |
|---------|--|------|------|
| copy | Copies a code image or a switch configuration to or from Flash memory or a TFTP server | PE | 3-20 |
| delete | Deletes a file or code image | PE | 3-22 |
| dir | Displays a list of files in Flash memory | PE | 3-23 |

| Command | Function | Mode | Page |
|-------------|---|------|------|
| whichboot | Displays the files booted | PE | 3-24 |
| boot system | Specifies the file or image used to start up the system | GC | 3-25 |

copy

Use this command to move (upload/download) a code image or configuration file between the switch's Flash memory and a TFTP server. When you save the system code or configuration settings to a file on a TFTP server, that file can later be downloaded to the switch to restore system operation. The success of the file transfer depends on the accessibility of the TFTP server and the quality of the network connection.

Syntax

```
copy file {file | running-config | startup-config | tftp}
copy running-config {file | startup-config | tftp}
copy startup-config {file | running-config | tftp}
copy tftp {file | running-config | startup-config}
```

- **file** - Keyword that allows you to copy to/from a file.
- **running-config** - Keyword that allows you to copy to/from the current running configuration.
- **startup-config** - The configuration used for system initialization.
- **tftp** - Keyword that allows you to copy to/from a TFTP server.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- The system prompts for data required to complete the copy command.
- The destination file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the TFTP server is 127 characters or 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")
- Due to the size limit of the Flash memory, the switch supports only one operation code file.
- The maximum number of user-defined configuration files depends on available memory.
- You can use "Factory_Default_Config.cfg" as the source to copy from the factory default configuration file, but you cannot use it as the destination.
- To replace the startup configuration, you must use **startup-config** as the destination.
- The Boot ROM image cannot be uploaded or downloaded from the TFTP server. You must use a direct console connection and access the download menu during a boot up to download the Boot ROM (or diagnostic) image. See "Upgrading Firmware via the Serial Port" on page B-1 for more details.

Example

The following example shows how to upload the configuration settings to a file on the TFTP server:

```
Console#copy file tftp
Choose file type:
 1. config:  2. opcode: <1-2>: 1
Source file name: startup
TFTP server ip address: 10.1.0.99
Destination file name: startup.01
TFTP completed.
Success.

Console#
```

The following example shows how to copy the running configuration to a startup file.

```
Console#copy running-config file
destination file name : startup
Write to FLASH Programming.
\Write to FLASH finish.
Success.
Console#
```

The following example shows how to download a configuration file:

```
Console#copy tftp startup-config
TFTP server ip address: 10.1.0.99
Source configuration file name: startup.01
Startup configuration file name [startup]:
Write to FLASH Programming.

\Write to FLASH finish.
Success.
Console#
```

delete

Use this command to delete a file or image.

Syntax

delete *filename*

filename - Name of the configuration file or image name.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- If the file type is used for system startup, then this file cannot be deleted.
- “Factory_Default_Config.cfg” cannot be deleted.

Example

This example shows how to delete the test2.cfg configuration file from Flash memory.

```
Console#delete test2.cfg
Console#
```

Related Commands

dir (3-23)

dir

Use this command to display a list of files in Flash memory.

Syntax

dir [**boot-rom** | **config** | **opcode** [:*filename*]]

The type of file or image to display includes:

- **boot-rom** - Boot ROM (or diagnostic) image file
- **config** - Switch configuration file
- **opcode** - Run-time operation code image file.
- *filename* - Name of the file or image. If this file exists but contains errors, information on this file cannot be shown.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- If you enter the command **dir** without any parameters, the system displays all files.
- File information is shown below:

| Column Heading | Description |
|----------------|--|
| file name | The name of the file. |
| file type | File types: Boot-Rom, Operation Code, and Config file. |
| startup | Shows if this file is used when the system is started. |
| size | The length of the file in bytes. |

Example

The following example shows how to display all file information:

| | | | | |
|-------------|----------------------------|----------------|---------|-------------|
| Console#dir | file name | file type | startup | size (byte) |
| | diag_0060 | Boot-Rom image | Y | 111360 |
| | run_0200 | Operation Code | Y | 1083008 |
| | Factory_Default_Config.cfg | Config File | N | 2574 |
| | startup | Config File | Y | 2710 |
| | Total free space: | | | 0 |
| Console# | | | | |

whichboot

Use this command to display which files booted.

Default Setting

None

Command Mode

Privileged Exec

Example

This example shows the information displayed by the **whichboot** command. See the table under the **dir** command for a description of the file information displayed by this command.

| Console#whichboot | | | | |
|-------------------|----------------|---------|-------------|--|
| file name | file type | startup | size (byte) | |
| diag_0060 | Boot-Rom image | Y | 111360 | |
| run_0200 | Operation Code | Y | 1083008 | |
| startup | Config File | Y | 2710 | |
| Console# | | | | |

boot system

Use this command to specify the file or image used to start up the system.

Syntax

boot system {boot-rom | config | opcode}: *filename*

The type of file or image to set as a default includes:

- **boot-rom** - Boot ROM
- **config** - Configuration file
- **opcode** - Run-time operation code

The colon (:) is required.

- *filename* - Name of the configuration file or image name.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- A colon (:) is required after the specified file type.
- If the file contains an error, it cannot be set as the default file.

Example

```
Console(config)#boot system config: startup
Console(config)#
```

Related Commands

- dir (3-23)
- whichboot (3-24)

System Management Commands

These commands are used to control system logs, passwords, user names, browser configuration options, and display or configure a variety of other system information.

| Command | Function | Mode | Page |
|----------------------------|--|------|------|
| Device Description Command | | | |
| hostname | Specifies or modifies the host name for the device | GC | 3-27 |
| User Access Commands | | | |
| username | Establishes a user name-based authentication system at login | GC | 3-27 |
| enable password | Sets a password to control access to the Privileged Exec level | GC | 3-29 |
| Web Server Commands | | | |
| ip http port | Specifies the port to be used by the Web browser interface | GC | 3-30 |
| ip http server | Allows the switch to be monitored or configured from a browser | GC | 3-31 |
| System Status Commands | | | |
| show startup-config | Displays the contents of the configuration file (stored in Flash memory) that is used to start up the system | PE | 3-32 |
| show running-config | Displays the configuration data currently in use | PE | 3-34 |

| Command | Function | Mode | Page |
|--------------|--|-----------|------|
| show system | Displays system information | NE, PE | 3-36 |
| show users | Shows all active console and Telnet sessions, including user name, idle time, and IP address of Telnet clients | NE, PE | 3-37 |
| show version | Displays version information for the system | NE, PE | 3-37 |

hostname

Use this command to specify or modify the host name for this device. Use the **no** form to restore the default host name.

Syntax

hostname *name*

no hostname

name - The name of this host. (Maximum length: 255 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#hostname noname
Console(config)#
```

username

Use this command to add named users, require authentication at login, specify or change a user's password (or specify that no password is required), or specify or change a user's access level. Use the **no** form to remove a user name.

Syntax

username *name* {**access-level** *level* | **nopassword** | **password** {**0** | **7**} *password*}

no username *name*

- *name* - The name of the user.
(Maximum length: 8 characters, case sensitive. Maximum users: 16)
- **access-level** *level* - Specifies the user level.
- The device has two predefined privilege levels:
0: Normal Exec, **15**: Privileged Exec.
- **nopassword** - No password is required for this user to log in.
- {**0** | **7**} - 0 means plain password, 7 means encrypted password.
- **password** *password* - The authentication password for the user. (Maximum length: 8 characters plain text, 32 encrypted, case sensitive)

Default Setting

- The default access level is Normal Exec.
- The factory defaults for the user names and passwords are:

| username | access-level | password |
|----------|--------------|----------|
| guest | 0 | guest |
| admin | 15 | admin |

Command Mode

Global Configuration

Command Usage

The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP server. There is no need for you to manually configure encrypted passwords.

Example

This example shows how to set the access level and password for a user.

```
Console(config)#username bob access-level 15
Console(config)#username bob password 0 smith
Console(config)#
```

enable password

After initially logging onto the system, you should set the Privileged Exec password. Remember to record it in a safe place. Use this command to control access to the Privileged Exec level from the Normal Exec level. Use the **no** form to reset the default password.

Syntax

enable password [*level level*] {**0** | **7**} *password*

no enable password [*level level*]

- **level level** - Level 15 for Privileged Exec. (Levels 0-14 are not used.)
- {**0** | **7**} - 0 means plain password, 7 means encrypted password.
- *password* - password for this privilege level.
(Maximum length: 8 characters plain text, 32 encrypted, case sensitive)

Default Setting

- The default is level 15.
- The default password is “super”

Command Mode

Global Configuration

Command Usage

- You cannot set a null password. You will have to enter a

password to change the command mode from Normal Exec to Privileged Exec with the **enable** command (page 3-13).

- The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP server. There is no need for you to manually configure encrypted passwords.

Example

```
Console(config)#enable password level 15 0 admin
Console(config)#
```

Related Commands

enable (3-13)

ip http port

Use this command to specify the TCP port number used by the Web browser interface. Use the **no** form to use the default port.

Syntax

ip http port *port-number*
no ip http port

port-number - The TCP port to be used by the browser interface. (Range: 1-65535)

Default Setting

80

Command Mode

Global Configuration

Example

```
Console(config)#ip http port 769
Console(config)#
```

Related Commands

ip http server (3-31)

ip http server

Use this command to allow this device to be monitored or configured from a browser. Use the **no** form to disable this function.

Syntax

ip http server

no ip http server

Default Setting

Enabled

Command Mode

Global Configuration

Example

```
Console(config)#ip http server
Console(config)#
```

Related Commands

ip http port (3-30)

show startup-config

Use this command to display the configuration file stored in non-volatile memory that is used to start up the system.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- Use this command in conjunction with the **show running-config** command to compare the information in running memory to the information stored in non-volatile memory.
- This command displays settings for key command modes. Each mode group is separated by “!” symbols, and includes the configuration mode command, and corresponding commands. This command displays the following information:
 - Users (names and access levels)
 - SNMP community strings
 - VLAN database (VLAN ID, name and state)
 - VLAN configuration settings for each interface
 - IP address of the default VLAN
 - Any configured settings for the console port and Telnet

Example

```
Console#show startup-config
building startup-config, please wait.....
!
username admin access-level 15
username admin password 0 admin
!
username guest access-level 0
username guest password 0 guest
!
enable password level 15 0 super
!
snmp community public ro
snmp community private rw
!
vlan database
  vlan 1 name DefaultVlan media ethernet state active
!
interface ethernet 1/1
  switchport allowed vlan add 1 untagged
  switchport native vlan 1
.
.
.
interface ethernet 1/26
  switchport allowed vlan add 1 untagged
  switchport native vlan 1
!
interface vlan 1
  ip address 10.1.0.1 255.255.255.0
!
!
line console
!
!line vty

end
Console#
```

Related Commands

show running-config (3-34)

show running-config

Use this command to display the configuration information currently in use.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- Use this command in conjunction with the **show startup-config** command to compare the information in running memory to the information stored in non-volatile memory.
- This command displays settings for key command modes. Each mode group is separated by “!” symbols, and includes the configuration mode command, and corresponding commands. This command displays the following information:
 - SNMP community strings
 - Users (names, access levels, and encrypted passwords)
 - VLAN database (VLAN ID, name and state)
 - VLAN configuration settings for each interface
 - IP address of configured VLAN
 - Any configured settings for the console port and Telnet

Example

```
Console#show running-config
building running-config, please wait.....
!
!
snmp-server community private rw
snmp-server community public ro
!
username admin access-level 15
username admin password 7 21232f297a57a5a743894a0e4a801fc3
username guest access-level 0
username guest password 7 084e0343a0486ff05530df6c705c8bb4
enable password level 15 7 1b3231655cebb7a1f783eddf27d254ca
!
vlan database
vlan 1 name DefaultVlan media ethernet state active.
!
!
interface ethernet 1/1
switchport allowed vlan add 1
switchport native vlan 1
switchport mode access
.
.
.
!
interface vlan 1
ip address 10.1.0.1 255.255.255.0
!
!
!
!
!
!
line console
!
!
line vty
!
!
!
end
Console#
```

Related Commands

show startup-config (3-32)

show system

Use this command to display system information.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

- For a description of the items shown by this command, refer to “Displaying System Information” on page -9.
- The POST results should all display “PASS.” If any POST test indicates “FAIL,” contact your distributor for assistance.

Example

```
Console#show system
System description: TigerSwitch 10/100 - 6724L2 Managed 24+2
  Standalone Switch
System OID string: 1.3.6.1.4.1.259.6.10.42
System information
  System Up time: 0 days, 3 hours, 53 minutes, and 31.79 seconds
  System Name      : [NONE]
  System Location   : [NONE]
  System Contact    : [NONE]
  MAC address       : 00-55-FF-FF-DD-DD
  Web server        : enable
  Web server port   : 80
  POST result

--- Performing Power-On Self Tests (POST) ---
UART Loopback Test.....PASS
Flash Memory Checksum Test.....PASS
CPU Self Test.....PASS
MPC850 clock Timer and Interrupt TEST...PASS
WatchDog Timer and Interrupt Test.....PASS
DRAM Test.....PASS
ACD Chip Test.....PASS
Switch Driver Initialization.....PASS
Switch Internal Loopback Test .....PASS
----- DONE -----
Console#
```

show users

Shows all active console and Telnet sessions, including user name, idle time, and IP address of Telnet client.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

The session used to execute this command is indicated by a "*" symbol next to the Line (i.e., session) index number.

Example

```

Console#show users
Username accounts:
Username Privilege
-----
      admin      15
      guest       0

Online users:
Line      Username Idle time (h:m:s) Remote IP addr.
-----
* 0   console   admin      0:00:00
  1   vty 0     admin      0:04:37      10.1.0.19
Console#

```

show version

Use this command to display hardware and software version information for the system.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

See “Displaying Switch Hardware/Software Versions” on page -28 for detailed information on software items. The meaning of hardware items are as follows:

- **Serial Number** – Serial number of the main board.
- **Hardware Version** – Hardware version of the main board.
- **Number of Ports** – Number of ports on this switch
- **Module Type** – The module type installed in this switch
- **Main Power Status** – Power status for the switch.

Example

```
Console#show version
Unit1
  Serial number      :12345
  Hardware version   :012
  Module A type      :not present
  Module B type      :not present
  Number of ports    :26
  Main power status  :up
Agent(master)
  Unit id            :1
  Loader version     :0.0.0.2
  Boot rom version   :0.0.0.6
  Operation code version :1.0.0.5
Console#
```

Authentication Commands

You can configure this switch to authenticate users logging into the system for management access using local or RADIUS authentication methods.

Remote Authentication Dial-in User Service (RADIUS) is a logon authentication protocol that uses software running on a central server to control access to RADIUS-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user that requires management access to a switch.

| Command | Function | Mode | Page |
|------------------------------|---|------|------|
| <i>Authentication Method</i> | | | |
| authentication login | Defines logon authentication method and precedence | GC | 3-39 |
| <i>RADIUS Client</i> | | | |
| radius-server host | Specifies the RADIUS server | GC | 3-40 |
| radius-server port | Sets the RADIUS server network port | GC | 3-41 |
| radius-server key | Sets the RADIUS encryption key | GC | 3-42 |
| radius-server retransmit | Sets the number of retries | GC | 3-42 |
| radius-server timeout | Sets the interval between sending authentication requests | GC | 3-43 |
| show radius-server | Shows the current RADIUS settings | PE | 3-43 |

authentication login

Use this command to define the login authentication method and precedence. Use the **no** form to restore the default.

Syntax

authentication login [[**local**] [**radius**]]

no authentication login

- **local** - Use local password only.
- **radius** - Use RADIUS server password only.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- RADIUS uses UDP which only offers best-effort delivery. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server.
- RADIUS logon authentication assigns a specific privilege level for each user name and password pair. The user name, password, and privilege level must be configured on the authentication server.
- You can specify two authentication methods in a single command to indicate the authentication sequence. For example, if you enter “**authentication login radius local**,” the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then the local user name and password is checked.

Example

```
Console(config)#authentication login radius
Console(config)#
```

Related Commands

username - for setting the local user names and passwords
(3-27)

radius-server host

Use this command to specify the RADIUS server. Use the **no** form to restore the default.

Syntax

radius-server host *host_ip_address*
no radius-server host

host_ip_address - IP address of server.

Default Setting

10.1.0.1

Command Mode

Global Configuration

Example

```
Console(config)#radius-server host 192.168.1.25  
Console(config)#
```

radius-server port

Use this command to set the RADIUS server network port. Use the **no** form to restore the default.

Syntax

radius-server port *port_number*
no radius-server port

port_number - RADIUS server UDP port used for authentication messages. (Range: 1-65535)

Default Setting

1812

Command Mode

Global Configuration

Example

```
Console(config)#radius-server port 181  
Console(config)#
```

radius-server key

Use this command to set the RADIUS encryption key. Use the **no** form to restore the default.

Syntax

radius-server key *key_string*
no radius-server key

key_string - Encryption key used to authenticate logon access for client. Do not use blank spaces in the string.
(Maximum length: 20 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#radius-server key green
Console(config)#
```

radius-server retransmit

Use this command to set the number of retries. Use the **no** form to restore the default.

Syntax

radius-server retransmit *number_of_retries*
no radius-server retransmit

number_of_retries - Number of times the switch will try to authenticate logon access via the RADIUS server.
(Range is 1 - 30)

Default Setting

2

Command Mode

Global Configuration

Example

```
Console(config)#radius-server retransmit 5
Console(config)#
```

radius-server timeout

Use this command to set the interval between transmitting authentication requests to the RADIUS server. Use the **no** form to restore the default.

Syntax**radius-server timeout** *number_of_seconds***no radius-server timeout**

number_of_seconds - Number of seconds the switch waits for a reply before resending a request. (Range: 1-65535)

Default Setting

5

Command Mode

Global Configuration

Example

```
Console(config)#radius-server timeout 10
Console(config)#
```

show radius-server

Use this command to display the current settings for the RADIUS server.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show radius-server
Server IP address: 10.1.0.99
  Communication key with radius server:
  Server port number: 1812
  Retransmit times: 2
  Request timeout: 5
Console#
```

Port Authentication Commands

The switch supports IEEE 802.1x (dot1x) port-based access control that prevents unauthorized access to the network by requiring users to first enter a user ID and password for authentication. Client authentication is controlled centrally by a RADIUS server using EAPOL (Extensible Authentication Protocol Over LAN).

| Command | Function | Mode | Page |
|----------------------------|--|------|------|
| authentication dot1x | Enables authentication on all switch ports by setting the dot1x mode to “Auto” | GC | 3-45 |
| dot1x default | Resets all dot1x parameters to their default values | GC | 3-46 |
| dot1x max-req | Sets the maximum number of requests the switch can send for the authentication process before starting the process again | GC | 3-46 |
| dot1x port-control | Sets dot1x mode for a port interface | IC | 3-47 |
| dot1x re-authenticate | Forces a re-authentication on specific ports | PE | 3-48 |
| dot1x re-authentication | Enables re-authentication for all ports | GC | 3-48 |

| Command | Function | Mode | Page |
|-----------------------------|--|------|------|
| dot1x timeout quiet-period | Sets the time that a switch port waits after the Max Request Count has been exceeded before attempting to acquire a new client | GC | 3-49 |
| dot1x timeout re-authperiod | Sets the time period after which a connected client must be re-authenticated | GC | 3-49 |
| dot1x timeout tx-period | Sets the time period during an authentication session that the switch waits before re-transmitting an EAP packet | GC | 3-50 |
| show dot1x | Shows all dot1x related information | PE | 3-51 |

authentication dot1x

Sets the default authentication server type. Use the **no** form to restore the default.

Syntax

authentication dot1x default radius
no authentication dot1x

Default Setting

RADIUS

Command Mode

Global Configuration

Example

```
Console(config)#authentication dot1x default radius
Console(config)#
```

dot1x default

Sets all configurable dot1x global and port settings to their default values.

Syntax

dot1x default

Command Mode

Global Configuration

Example

```
Console(config)#dot1x default
Console(config)#
```

dot1x max-req

Sets the maximum number of times the switch port will retransmit an EAP request packet to the client before it times out the authentication session. Use the **no** form to restore the default.

Syntax

dot1x max-req *count*
no dot1x max-req

count – Maximum number of requests. (Range: 1 - 10)

Default

2

Command Mode

Global Configuration

Example

```
Console(config)#dot1x max-req 2
Console(config)#
```

dot1x port-control

Sets the dot1x mode on a port interface. Use the **no** form to reset to the default.

Syntax

**dot1x port-control {auto | force-authorized |
force-unauthorized}
no dot1x port-control**

- **auto** – Requires a dot1x-aware connected client to be authorized by the RADIUS server. Clients that are not dot1x-aware will be denied access.
- **force-authorized** – Configures the port to grant access to all clients, either dot1x-aware or otherwise.
- **force-unauthorized** – Configures the port to deny access to all clients, either dot1x-aware or otherwise.

Default

force-authorized

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2  
Console(config-if)#dot1x port-control auto  
Console(config-if)#
```

dot1x re-authenticate

Forces re-authentication on all ports or a specific interface.

Syntax

dot1x re-authenticate [*interface*]

interface

- **ethernet** *unit/port*
 - *unit* - This is device 1.
 - *port* - Port number.

Command Mode

Privileged Exec

Example

```
Console#dot1x re-authenticate
Console#
```

dot1x re-authentication

Enables periodic re-authentication globally for all ports. Use the **no** form to disable re-authentication.

Syntax

dot1x re-authentication
no dot1x re-authentication

Command Mode

Global Configuration

Example

```
Console(config)#dot1x re-authentication
Console(config)#
```

dot1x timeout quiet-period

Sets the time that a switch port waits after the Max Request Count has been exceeded before attempting to acquire a new client. Use the **no** form of this command to reset the default.

Syntax

dot1x timeout quiet-period *seconds*
no dot1x timeout quiet-period *seconds*

seconds - Number of seconds. (Range: 0-65535 seconds)

Default

60 seconds

Command Mode

Global Configuration

Example

```
Console(config)#dot1x timeout quiet-period 350  
Console(config)#
```

dot1x timeout re-authperiod

Sets the time period after which a connected client must be re-authenticated.

Syntax

dot1x timeout re-authperiod *seconds*
no dot1x timeout re-authperiod

seconds - Number of seconds. (Range: 0-65535 seconds)

Default

3600 seconds

Command Mode

Global Configuration

Example

```
Console(config)#dot1x timeout re-authperiod 300
Console(config)#
```

dot1x timeout tx-period

Sets the time period during an authentication session that the switch waits before re-transmitting an EAP packet. Use the **no** form to reset to the default value.

Syntax

dot1x timeout tx-period *seconds*

no dot1x timeout tx-period

seconds - Number of seconds. (Range: 1-65535 seconds)

Default

30 seconds

Command Mode

Global Configuration

Example

```
Console(config)#dot1x timeout tx-period 300
Console(config)#
```


show dot1x

Use this command to show general port authentication related settings on the switch or a specific interface.

Syntax

show dot1x [**statistics**] [**interface** *interface*]

interface

- **ethernet** *unit/port*
 - *unit* - This is device 1.
 - *port* - Port number.

Command Mode

Privileged Exec

Command Usage

This command displays the following information:

- *Global 802.1X Parameters* – Displays the global port access control parameters that can be configured for this switch as described in the preceeding pages, including reauth-enabled (page 3-48), reauth-period (page 3-49), quiet-period (page 3-49), tx-period (page 3-50), and max-req (page 3-46). It also displays the following global parameters which are set to a fixed value, including the following items:
 - supp-timeout– Supplicant timeout.
 - server-timeout– Server timeout.
 - reauth-max– Maximum number of reauthentication attempts.
- *802.1X Port Summary* – Displays the port access control parameters for each interface, including the following items:
 - Status– Administrative state for port access control.
 - Mode– Dot1x port control mode (page 3-47).
 - Authorized– Authorization status (yes or n/a - not authorized).

- *802.1X Port Details* – Displays detailed port access control settings for each interface as described in the preceeding pages, including administrative status for port access control, Max request (page 3-46), Quiet period (page 3-49), Reauth period (page 3-49), Tx period (page 3-50), and Port-control (page 3-47). It also displays the following information:
 - Status– Authorization status (authorized or unauthorized).
 - Supplicant– MAC address of authorized client.
- *Authenticator State Machine*
 - State– Current state (including initialize, disconnected, connecting, authenticating, authenticated, aborting, held, force_authorized, force_unauthorized).
 - Reauth Count– Number of times connecting state is re-entered.
- *Backend State Machine*
 - State– Current state (including request, response, success, fail, timeout, idle, initialize).
 - Request Count– Number of EAP Request packets sent to the Supplicant without receiving a response.
 - Identifier(Server)– Identifier carried in the most recent EAP Success, Failure or Request packet received from the Authentication Server.
- *Reauthentication State Machine*
 - State– Current state (including initialize, reauthenticate).

Example

```

Console#show dot1x
Global 802.1X Parameters
reauth-enabled: yes
reauth-period: 3600
quiet-period: 350
tx-period: 300
supp-timeout: 30
server-timeout: 30
reauth-max: 2
max-req: 2

802.1X Port Summary
  Port Name      Status      Mode      Authorized
    1          disabled ForceAuthorized n/a
    2           enabled      Auto      n/a
    .....
   25          disabled ForceAuthorized n/a
   26          disabled ForceAuthorized yes
   27          disabled ForceAuthorized yes

802.1X Port Details

802.1X is disabled on port 1

802.1X is enabled on port 2
Max request      2
Quiet period     350
Reauth period    3600
Tx period        300
Status           Unauthorized
Port-control     Auto
Supplicant       00-00-00-00-00-00

Authenticator State Machine
State            Connecting
Reauth Count     3

Backend State Machine
State            Idle
Request Count    0
Identifier(Server) 0

Reauthentication State Machine
State            Initialize

802.1X is disabled on port 4
.....
802.1X is disabled on port 25

802.1X is disabled on port 26

802.1X is disabled on port 27
Console#

```

SNMP Commands

Controls access to this switch from management stations using the Simple Network Management Protocol (SNMP), as well as the error types sent to trap managers.

| Command | Function | Mode | Page |
|--------------------------|---|--------|------|
| snmp-server community | Sets up the community access string to permit access to SNMP commands | GC | 3-54 |
| snmp-server contact | Sets the system contact string | GC | 3-55 |
| snmp-server location | Sets the system location string | GC | 3-56 |
| snmp-server host | Specifies the recipient of an SNMP notification operation | GC | 3-57 |
| snmp-server enable traps | Enables the device to send SNMP traps or inform requests (i.e., SNMP notifications) | GC | 3-58 |
| show snmp | Displays the status of SNMP communications | NE, PE | 3-59 |

snmp-server community

Use this command to define the community access string for the Simple Network Management Protocol. Use the **no** form to remove the specified community string.

Syntax

snmp-server community *string* [**ro** | **rw**]
no snmp-server community *string*

- *string* - Community string that acts like a password and permits access to the SNMP protocol. (Maximum length: 32 characters, case sensitive; Maximum number of strings: 5)
- **ro** - Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.

- **rw** - Specifies read-write access. Authorized management stations are able to both retrieve and modify MIB objects.

Default Setting

- **public** - Read-only access. Authorized management stations are only able to retrieve MIB objects.
- **private** - Read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

Command Mode

Global Configuration

Command Usage

The first **snmp-server community** command you enter enables SNMP (SNMPv1). The **no snmp-server community** command disables SNMP.

Example

```
Console(config)#snmp-server community alpha rw
Console(config)#
```

snmp-server contact

Use this command to set the system contact string. Use the **no** form to remove the system contact information.

Syntax

snmp-server contact *string*
no snmp-server contact

string - String that describes the system contact information.
 (Maximum length: 255 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#snmp-server contact Geoff
Console(config)#
```

Related Commands

snmp-server location

snmp-server location

Use this command to set the system location string. Use the **no** form to remove the location string.

Syntax

snmp-server location *text*
no snmp-server location

text - String that describes the system location.
(Maximum length: 255 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#snmp-server location TPS - 3rd Floor
Console(config)#
```

Related Commands

snmp-server contact (3-55)

snmp-server host

Use this command to specify the recipient of a Simple Network Management Protocol notification operation. Use the **no** form to remove the specified host.

Syntax

snmp-server host *host-addr community-string version*
version-number

no snmp-server host *host-addr*

- *host-addr* - Name or Internet address of the host (the targeted recipient). (Maximum host addresses: 5 trap destination IP address entries)
- *community-string* - Password-like community string sent with the notification operation. Though you can set this string using the **snmp-server host** command by itself, we recommend you define this string using the **snmp-server community** command prior to using the **snmp-server host** command. (Maximum length: 32 characters)
- **version-number** - {1 | 2c} indicates if the host is running SNMP version 1 or version 2c.

Default Setting

None

Command Mode

Global Configuration

Command Usage

If you do not enter an **snmp-server host** command, no notifications are sent. In order to configure the switch to send SNMP notifications, you must enter at least one **snmp-server host** command. In order to enable multiple hosts, you must issue a separate **snmp-server host** command for each host.

The **snmp-server host** command is used in conjunction with the **snmp-server enable traps** command. Use the **snmp-server enable traps** command to specify which SNMP notifications are sent globally. For a host to receive notifications, at least one **snmp-server enable traps** command and the **snmp-server host** command for that host must be enabled.

However, some notification types cannot be controlled with the **snmp-server enable traps** command. For example, some notification types are always enabled.

Example

```
Console(config)#snmp-server host 10.1.19.23 batman version 1
Console(config)#
```

Related Commands

snmp-server enable traps (3-58)

snmp-server enable traps

Use this command to enable this device to send Simple Network Management Protocol traps or informs (SNMP notifications). Use the **no** form to disable SNMP notifications.

Syntax

snmp-server enable traps [authentication | link-up-down]
no snmp-server enable traps [authentication | link-up-down]

- **authentication** - Keyword to issue authentication failure traps.
- **link-up-down** - Keyword to issue link-up or link-down traps.

The link-up-down trap can only be enabled/disabled via the CLI.

Default Setting

Issue authentication and link-up-down traps.

Command Mode

Global Configuration

Command Usage

If you do not enter an **snmp-server enable traps** command, no notifications controlled by this command are sent. In order to configure this device to send SNMP notifications, you must enter at least one **snmp-server enable traps** command. If you enter the command with no keywords, both authentication and link-up-down notifications are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled.

The **snmp-server enable traps** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. In order to send notifications, you must configure at least one **snmp-server host** command.

Example

```
Console(config)#snmp-server enable traps link-up-down
Console(config)#
```

Related Commands

snmp-server host (3-57)

show snmp

Use this command to check the status of SNMP communications.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

This command provides information on the community access strings, counter information for SNMP input and output protocol data units, and whether or not SNMP logging has been enabled with the **snmp-server enable traps** command.

Example

```
SNMP traps:
  Authentication: enable
  Link-up-down: enable

SNMP communities:
  1. private, and the privilege is read-write
  2. public, and the privilege is read-only

0 SNMP packets input
  0 Bad SNMP version errors
  0 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
  0 Number of requested variables
  0 Number of altered variables
  0 Get-request PDUs
  0 Get-next PDUs
  0 Set-request PDUs
0 SNMP packets output
  0 Too big errors
  0 No such name errors
  0 Bad values errors
  0 General errors
  0 Response PDUs
  0 Trap PDUs

SNMP logging: disabled
Console#
```

IGMP Snooping Commands

This switch uses IGMP (Internet Group Management Protocol) to query for any attached hosts that want to receive a specific multicast service. It identifies the ports containing hosts requesting a service and sends data out to those ports only. It then propagates the service request up to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service.

| Command | Function | Mode | Page |
|--|--|------|------|
| ip igmp snooping | Enables IGMP snooping | GC | 3-61 |
| ip igmp snooping query-count | Configures the query count | GC | 3-62 |
| ip igmp snooping query-max-response-time | Configures the report delay | GC | 3-63 |
| ip igmp snooping router-port-expire-time | Configures the query timeout | GC | 3-64 |
| ip igmp snooping version | Configures the IGMP version for snooping | GC | 3-65 |
| show ip igmp snooping | Shows the IGMP snooping configuration | PE | 3-66 |
| show mac-address-table multicast | Shows the IGMP snooping MAC multicast list | PE | 3-67 |

ip igmp snooping

Use this command to enable IGMP snooping on this switch. Use the **no** form to disable it.

Syntax

ip igmp snooping
no ip igmp snooping

Default Setting

Enabled

Command Mode

Global Configuration

Example

The following example enables IGMP snooping.

```
Console(config)#ip igmp snooping
Console(config)#
```

ip igmp snooping query-count

Use this command to configure the query count. Use the **no** form to restore the default.

Syntax

ip igmp snooping query-count *count*
no ip igmp snooping query-count

count - The maximum number of queries issued for which there has been no response before the switch takes action to drop a client from the multicast group. (Range: 2-10)

Default Setting

2 times

Command Mode

Global Configuration

Command Usage

The query count defines how long the querier waits for a response from a multicast client before taking action. If a querier has sent a number of queries defined by this command, but a client has not responded, a countdown timer is started using the time defined by **ip igmp snooping query-max-**

response-time. If the countdown finishes, and the client still has not responded, then that client is considered to have left the multicast group.

Example

The following shows how to configure the query count to 10:

```
Console(config)#ip igmp snooping query-count 10
Console(config)#
```

Related Commands

ip igmp snooping query-max-response-time (3-63)

ip igmp snooping query-max-response-time

Use this command to configure the snooping report delay. Use the **no** form of this command to restore the default.

Syntax

ip igmp snooping query-max-response-time *seconds*
no ip igmp snooping query-max-response-time

seconds - The report delay advertised in IGMP queries.
(Range: 5-30)

Default Setting

10 seconds

Command Mode

Global Configuration

Command Usage

- The switch must be using IGMPv2 for this command to take effect.
- This command defines the time after a query, during which a response is expected from a multicast client. If a querier has sent a number of queries defined by the **ip igmp snooping**

query-count, but a client has not responded, a countdown timer is started using an initial value set by this command. If the countdown finishes, and the client still has not responded, then that client is considered to have left the multicast group.

Example

The following shows how to configure the maximum response time to 20 seconds:

```
Console(config)#ip igmp snooping query-max-response-time 20
Console(config)#
```

Related Commands

ip igmp snooping version (3-65)

ip igmp snooping router-port-expire-time

Use this command to configure the snooping query timeout. Use the **no** form of this command to restore the default.

Syntax

ip igmp snooping router-port-expire-time *seconds*
no ip igmp snooping router-port-expire-time

seconds - The time the switch waits after the previous querier stops before it considers the router port (i.e., the interface which had been receiving query packets) to have expired.

(Range: 300-500)

Default Setting

300 seconds

Command Mode

Global Configuration

Command Usage

The switch must be using IGMPv2 for this command to take effect.

Example

The following shows how to configure the default timeout to 300 seconds:

```
Console(config)#ip igmp snooping router-port-expire-time 300
Console(config)#
```

Related Commands

ip igmp snooping version (3-65)

ip igmp snooping version

Use this command to configure the IGMP snooping version. Use the **no** form to restore the default.

Syntax

ip igmp snooping version {1 | 2}
no ip igmp snooping version

- **1** - IGMP Version 1
- **2** - IGMP Version 2

Default Setting

IGMP Version 2

Command Mode

Global Configuration

Command Usage

- All systems on the subnet must support the same version. If there are legacy devices in your network that only support Version 1, you will also have to configure this switch to use Version 1.

- Some commands are only enabled for IGMPv2, including **ip igmp query-max-response-time** and **ip igmp query-timeout**.

Example

The following configures the switch to use IGMP Version 1:

```
Console(config)#ip igmp snooping version 1
Console(config)#
```

show ip igmp snooping

Use this command to show the IGMP snooping configuration.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

See “Configuring IGMP Snooping Parameters” for a description of the displayed items.

Example

The following shows the current IGMP snooping configuration:

```
Console#show ip igmp snooping
Service status: Enabled
Query count: 2
Query max response time: 10 sec
Router port expire time: 300 sec
IGMP snooping version: Version 2
Console#
```


show mac-address-table multicast

Use this command to show known multicast addresses.

Syntax

show mac-address-table multicast [**vlan** *vlan-id*]
[user | igmp-snooping]

- *vlan-id* - VLAN ID (1 to 4094)
- **user** - Display only the user-configured multicast entries.
- **igmp-snooping** - Display only entries learned through IGMP snooping.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Member types displayed include IGMP or USER, depending on selected options.

Example

The following shows the multicast entries learned through IGMP snooping for bridge group 1, VLAN 1:

```
Console#show mac-address-table multicast vlan 1 igmp-snooping
VLAN M'cast IP addr. Member ports Type
-----
1      224.1.1.2.3      Eth1/11      IGMP
Console#
```

Line Commands

You can access the onboard configuration program by attaching a VT100 compatible device to the server's serial port. These commands are used to set communication parameters for the serial port or Telnet (i.e., a virtual terminal).

| Command | Function | Mode | Page |
|-----------------|--|--------|------|
| line | Identifies a specific line for configuration and starts the line configuration mode | GC | 3-69 |
| login | Enables password checking at login | LC | 3-70 |
| password | Specifies a password on a line | LC | 3-71 |
| exec-timeout | Sets the interval that the command interpreter waits until user input is detected | LC | 3-72 |
| password-thresh | Sets the password intrusion threshold, which limits the number of failed logon attempts | LC | 3-73 |
| silent-time* | Sets the amount of time the management console is inaccessible after the number of unsuccessful logon attempts exceeds the threshold set by the password-thresh command | LC | 3-74 |
| databits* | Sets the number of data bits per character that are interpreted and generated by hardware | LC | 3-75 |
| parity* | Defines the generation of a parity bit | LC | 3-76 |
| speed* | Sets the terminal baud rate | LC | 3-77 |
| stopbits* | Sets the number of the stop bits transmitted per byte | LC | 3-78 |
| show line | Displays a terminal line's parameters | NE, PE | 3-78 |

** These commands only apply to the serial port.*

line

Use this command to identify a specific line for configuration, and to process subsequent line configuration commands.

Syntax

line {**console** | **vty**}

- **console** - Console terminal line.
- **vty** - Virtual terminal for remote console access.

Default Setting

There is no default line.

Command Mode

Global Configuration

Command Usage

Telnet is considered a virtual terminal connection and will be shown as “Vty” in screen displays such as **show users**.

However, the serial communication parameters (e.g., databits) do not affect Telnet connections.

Example

To enter console line mode, enter the following command:

```
Console(config)#line console
Console(config-line)#
```

Related Commands

show line (3-78)
show users (3-37)

login

Use this command to enable password checking at login. Use the **no** form to disable password checking and allow connections without a password.

Syntax

login [**local**]

no login

local - Selects local password checking. Authentication is based on the user name specified with the **username** command.

Default Setting

login local

Command Mode

Line Configuration

Command Usage

- There are three authentication modes provided by the switch itself at login:
 - **login** selects authentication by a single global password as specified by the **password** line configuration command. When using this method, the management interface starts in Normal Exec (NE) mode.
 - **login local** selects authentication via the user name and password specified by the **username** command (i.e., default setting). When using this method, the management interface starts in Normal Exec (NE) or Privileged Exec (PE) mode, depending on the user's privilege level (0 or 15 respectively).
 - **no login** selects no authentication. When using this method, the management interface starts in Normal Exec (NE) mode.

- This command controls login authentication via the switch itself. To configure user names and passwords for remote authentication servers, you must use the RADIUS software installed on those servers.

Example

```
Console(config-line)#login local
Console(config-line)#
```

Related Commands

username (3-27)

password (3-71)

password

Use this command to specify the password for a line. Use the **no** form to remove the password.

Syntax

password {0 | 7} *password*

no password

- {0 | 7} - 0 means plain password, 7 means encrypted password
- *password* - Character string that specifies the line password. (Maximum length: 8 characters plain text, 32 encrypted, case sensitive)

Default Setting

No password is specified.

Command Mode

Line Configuration

Command Usage

- When a connection is started on a line with password protection, the system prompts for the password. If you enter the correct password, the system shows a prompt. You can use the **password-thresh** command to set the number of times a user can enter an incorrect password before the system terminates the line connection and returns the terminal to the idle state.
- The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP server. There is no need for you to manually configure encrypted passwords.

Example

```
Console(config-line)#password 0 secret
Console(config-line)#
```

Related Commands

login (3-70)

password-thresh (3-73)

exec-timeout

Use this command to set the interval that the system waits until user input is detected. Use the **no** form to restore the default.

Syntax

exec-timeout *seconds*

no exec-timeout

seconds - Integer that specifies the number of seconds.
(Range: 0 - 65535 seconds; 0: no timeout)

Default Setting

CLI: No timeout

Telnet: 10 minutes

Command Mode

Line Configuration

Command Usage

- If user input is detected within the timeout interval, the session is kept open; otherwise the session is terminated.
- This command applies to both the local console and Telnet connections.
- The timeout for Telnet cannot be disabled.

Example

To set the timeout to two minutes, enter this command:

```
Console(config-line)#exec-timeout 120  
Console(config-line)#
```

password-thresh

Use this command to set the password intrusion threshold which limits the number of failed logon attempts. Use the **no** form to remove the threshold value.

Syntax

password-thresh *threshold*

no password-thresh

threshold - The number of allowed password attempts.
(Range: 1-120; 0: no threshold)

Default Setting

The default value is three attempts.

Command Mode

Line Configuration

Command Usage

- When the logon attempt threshold is reached, the system interface becomes silent for a specified amount of time before allowing the next logon attempt. (Use the **silent-time** command to set this interval.) When this threshold is reached for Telnet, the Telnet logon interface shuts down.
- This command applies to both the local console and Telnet connections.

Example

To set the password threshold to five attempts, enter this command:

```
Console(config-line)#password-thresh 5
Console(config-line)#
```

Related Commands

silent-time (3-74)

silent-time

Use this command to set the amount of time the management console is inaccessible after the number of unsuccessful logon attempts exceeds the threshold set by the **password-thresh** command. Use the **no** form to remove the silent time value.

Syntax

silent-time *seconds*

no silent-time

seconds - The number of seconds to disable console response. (Range: 0-65535; 0: no silent-time)

Default Setting

The default value is no silent-time.

Command Mode

Line Configuration

Example

To set the silent time to 60 seconds, enter this command:

```
Console(config-line)#silent-time 60
Console(config-line)#
```

Related Commands

password-thresh (3-73)

databits

Use this command to set the number of data bits per character that are interpreted and generated by the console port. Use the **no** form to restore the default value.

Syntax

databits {7 | 8}

no databits

- 7 - Seven data bits per character.
- 8 - Eight data bits per character.

Default Setting

8 data bits per character

Command Mode

Line Configuration

Command Usage

The **databits** command can be used to mask the high bit on input from devices that generate 7 data bits with parity. If parity is being generated, specify 7 data bits per character. If no parity is required, specify 8 data bits per character.

Example

To specify 7 data bits, enter this command:

```
Console(config-line)#databits 7
Console(config-line)#
```

Related Commands

parity (3-76)

parity

Use this command to define generation of a parity bit. Use the **no** form to restore the default setting.

Syntax

parity {**none** | **even** | **odd**}
no parity

- **none** - No parity
- **even** - Even parity
- **odd** - Odd parity

Default Setting

No parity

Command Mode

Line Configuration

Command Usage

Communication protocols provided by devices such as terminals and modems often require a specific parity bit setting.

Example

To specify no parity, enter this command:

```
Console(config-line)#parity none
Console(config-line)#
```

speed

Use this command to set the terminal line's baud rate. This command sets both the transmit (to terminal) and receive (from terminal) speeds. Use the **no** form to restore the default setting.

Syntax

speed *bps*

no speed

bps - Baud rate in bits per second.

(Options: 9600, 57600, 38400, 19200, 115200 bps)

Default Setting

9600 bps

Command Mode

Line Configuration

Command Usage

Set the speed to match the baud rate of the device connected to the serial port. Some baud rates available on devices connected to the port might not be supported. The system indicates if the speed you selected is not supported.

Example

To specify 57600 bps, enter this command:

```
Console(config-line)#speed 57600
Console(config-line)#
```

stopbits

Use this command to set the number of the stop bits transmitted per byte. Use the **no** form to restore the default setting.

Syntax

stopbits {**1** | **2**}

- **1** - One stop bit
- **2** - Two stop bits

Default Setting

1 stop bit

Command Mode

Line Configuration

Example

To specify 2 stop bits, enter this command:

```
Console(config-line)#stopbits 2
Console(config-line)#
```

show line

Use this command to display the terminal line's parameters.

Syntax

show line [**console** | **vty**]

- **console** - Console terminal line.
- **vty** - Virtual terminal for remote console access.

Default Setting

Shows all lines

Command Mode

Normal Exec, Privileged Exec

Example

To show all lines, enter this command:

```

Console#show line
Console configuration:
  Password threshold: 3 times
  Interactive timeout: Disabled
  Silent time: Disabled
  Baudrate: 9600
  Databits: 8
  Parity: none
  Stopbits: 1

Vty configuration:
  Password threshold: 3 times
  Interactive timeout: 65535
Console#

```

IP Commands

There are no IP addresses assigned to this switch by default. You must manually configure a new address to manage the switch over your network. You may also need to establish a default gateway between this device and management stations that exist on another network segment.

| Command | Function | Mode | Page |
|--------------------|---|--------|------|
| ip address | Sets the IP address for this device | IC | 3-80 |
| ip dhcp restart | Submits a BOOTP or DHCP client request | PE | 3-81 |
| ip default-gateway | Defines the default gateway through which an in-band management station can reach this device | GC | 3-82 |
| show ip interface | Displays the IP settings for this device | PE | 3-83 |
| show ip redirects | Displays the default gateway configured for this device | PE | 3-84 |
| ping | Sends ICMP echo request packets to another node on the network | NE, PE | 3-84 |

ip address

Use this command to set the IP address for this device. Use the **no** form to restore the default IP address.

Syntax

ip address {*ip-address netmask* | **bootp** | **dhcp**}
no ip address

- *ip-address* - IP address
- *netmask* - Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- **bootp** - Obtains IP address from BOOTP.
- **dhcp** - Obtains IP address from DHCP.

Default Setting

IP address: 0.0.0.0

Netmask: 255.0.0.0

Command Mode

Interface Configuration (VLAN)

Command Usage

- You must assign an IP address to this device to gain management access over the network. You can manually configure a specific IP address, or direct the device to obtain an address from a BOOTP or DHCP server. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Anything outside this format will not be accepted by the configuration program.
- If you select the **bootp** or **dhcp** option, IP is enabled but will not function until a BOOTP or DHCP reply has been received. Requests will be broadcast periodically by this device in an effort to learn its IP address. (BOOTP and DHCP values can include the IP address, default gateway, and subnet mask).

- You can start broadcasting BOOTP or DHCP requests by entering an **ip dhcp restart** command, or by rebooting the switch.

Note: Only one VLAN interface can be assigned an IP address (the default is VLAN 1). This defines the management VLAN, the only VLAN through which you can gain management access to the switch. If you assign an IP address to any other VLAN, the new IP address overrides the original IP address and this becomes the new management VLAN.

Example

In the following example, the device is assigned an address in VLAN 1.

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.5 255.255.255.0
Console(config-if)#
```

Related Commands

ip dhcp restart (3-81)

ip dhcp restart

Use this command to submit a BOOTP or DHCP client request.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- DHCP requires the server to reassign the client's last address if available.

- If the BOOTP or DHCP server has been moved to a different domain, the network portion of the address provided to the client will be based on this new domain.

Example

In the following example, the device is reassigned the same address.

```
Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
Console(config-if)#exit
Console#ip dhcp restart
Console#show ip interface
IP interface vlan
  IP address and netmask: 10.1.0.54 255.255.255.0 on VLAN 1,
  and address mode: Dhcp.
Console#
```

Related Commands

ip address (3-80)

ip default-gateway

Use this command to establish a static route between this device and management stations that exist on another network segment. Use the **no** form to remove the static route.

Syntax

ip default-gateway *gateway*

no ip default-gateway

gateway - IP address of the default gateway

Default Setting

No static route is established.

Command Mode

Global Configuration

Command Usage

A gateway must be defined if the management station is located in a different IP segment.

Example

The following example defines a default gateway for this device:

```
Console(config)#ip default-gateway 10.1.0.254
Console(config)#
```

Related Commands

show ip redirects (3-84)

show ip interface

Use this command to display the settings of an IP interface.

Default Setting

All interfaces

Command Mode

Privileged Exec

Command Usage

This switch can only be assigned one IP address. This address is used for managing the switch.

Example

```
Console#show ip interface
IP address and netmask: 10.1.0.54 255.255.255.0 on VLAN 1,
and address mode: User specified.
Console#
```

Related Commands

show ip redirects (3-84)

show ip redirects

Use this command to show the default gateway configured for this device.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show ip redirects
ip default gateway 10.1.0.254
Console#
```

Related Commands

ip default-gateway (3-82)

ping

Use this command to send ICMP echo request packets to another node on the network.

Syntax

ping *host* [**count** *count*][**size** *size*]

- *host* - IP address or IP alias of the host.
- *count* - Number of packets to send. (Range: 1-16, default: 5)
- *size* - Number of bytes in a packet. (Range: 32-512, default: 32)

The actual packet size will be eight bytes larger than the size specified because the switch adds header information.

Default Setting

This command has no default for the host.

Command Mode

Normal Exec, Privileged Exec

Command Usage

- Use the ping command to see if another site on the network can be reached.
- Following are some results of the **ping** command:
 - *Normal response* - The normal response occurs in one to ten seconds, depending on network traffic.
 - *Destination does not respond* - If the host does not respond, a “no answer from host” appears in ten seconds.
 - *Destination unreachable* - The gateway for this destination indicates that the destination is unreachable.
 - *Network or host unreachable* - The gateway found no corresponding entry in the route table.
- Press <Esc> to stop pinging.

Example

```
Console#ping 10.1.0.9
Type ESC to abort.
PING to 10.1.0.9, by 5 32-byte payload ICMP packets, timeout is 5
seconds
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 0 ms
Ping statistics for 10.1.0.9:
 5 packets transmitted, 5 packets received (100%), 0 packets lost (0%)
Approximate round trip times:
  Minimum = 0 ms, Maximum = 10 ms, Average = 8 ms
Console#
```

Related Commands

interface (3-89)

HOL Blocking Prevention Commands

If head-of-line (HOL) Blocking Prevention is enabled it prevents the forwarding of data to a port transmit queue that is blocked. This allows for a more efficient transfer of packets across the network. Normally, when the switch sends traffic to a port it goes to the port's transmit queue and is then sent out. If the port's transmit queue is already busy trying to send out data then the switch will keep the waiting traffic in the queue until the port is ready to send it out.

However, if the port remains busy, the switch will fill up more of the transmit queue with traffic waiting to be sent out that port. HOL Blocking Prevention works on the assumption that it is better to randomly drop traffic waiting in the queue than to continue using more memory and impacting performance across all the ports.

The switch controls the maximum number of frames that can be accumulated in the transmit queue before frames are dropped.

Note: If HOL Blocking is enabled on this switch, priority tags cannot be processed.

| Command | Function | Mode | Page |
|---------------------------|---------------------------------|------|------|
| queue hol-prevention | Enables HOL Blocking Prevention | GC | 3-86 |
| show queue hol-prevention | Configures the query count | PE | 3-87 |

queue hol-prevention

Use this command to enable HOL Blocking Prevention. Use the no form of this command to disable it.

Syntax

queue hol-prevention
no queue hol-prevention

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

- If HOL Blocking Prevention is disabled on this switch. The transmit queue may be completely filled with frames awaiting service.
- If enabled, once the number of packets in the queue reaches a certain threshold, the switch will begin to randomly drop packets.

Example

The following example enables HOL Blocking Prevention.

```
Console(config)#queue hol-prevention  
Console(config)#
```

show queue hol-prevention

Use this command to show head-of-line (HOL) Blocking Prevention configuration.

Syntax

show queue hol-prevention

Command Mode

Privileged Exec

Example

This example displays the current status.

```
Console#show queue hol-prevention
HOL blocking prevention status: Disabled
Console#
```

Interface Commands

These commands are used to display or set communication parameters for an Ethernet port, aggregated link, or VLAN.

| Command | Function | Mode | Page |
|------------------------------------|---|-----------|------|
| interface | Configures an interface type and enters interface configuration mode | GC | 3-89 |
| description | Adds a description to an interface configuration | IC | 3-90 |
| speed-duplex | Configures the speed and duplex operation of a given interface when autonegotiation is disabled | IC | 3-90 |
| negotiation | Enables autonegotiation of a given interface | IC | 3-92 |
| capabilities | Advertises the capabilities of a given interface for use in autonegotiation | IC | 3-93 |
| flowcontrol | Enables flow control on a given interface | IC | 3-94 |
| shutdown | Disables an interface | IC | 3-96 |
| switchport broadcast percent | Configures broadcast storm control | IC | 3-97 |
| clear counters | Clears the statistics on the specified interface | PE | 3-98 |
| show interfaces status | Displays status for the specified interface | NE, PE | 3-99 |

| Command | Function | Mode | Page |
|----------------------------------|--|-----------|-------|
| show interfaces counters | Displays statistics for the specified interface | NE, PE | 3-100 |
| show interfaces switchport | Displays the administrative and operational status of an interface | NE, PE | 3-102 |

interface

Use this command to configure an interface type and enter interface configuration mode. Use the **no** form to remove a trunk.

Syntax

interface *interface*

no interface port-channel *channel-id*

interface

- **ethernet** *unit/port*
 - *unit* - This is device 1.
 - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-4)
- **vlan** *vlan-id* (Range: 1-4094)

Default Setting

None

Command Mode

Global Configuration

Example

To specify port 25, enter the following command:

```
Console(config)#interface ethernet 1/25
Console(config-if)#
```

description

Use this command to add a description to an interface. Use the **no** form to remove the description.

Syntax

description *string*

no description

string - Comment or a description to help you remember what is attached to this interface. (Range: 1-64 characters)

Default Setting

None

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

The following example adds a description to port 25.

```
Console(config)#interface ethernet 1/25
Console(config-if)#description RD-SW#3
Console(config-if)#
```

speed-duplex

Use this command to configure the speed and duplex mode of a given interface when autonegotiation is disabled. Use the **no** form to restore the default.

Syntax

speed-duplex {**1000full** | **100full** | **100half** | **10full** | **10half**}

no speed-duplex

- **1000full** - Forces 1000 Mbps full-duplex operation
- **100full** - Forces 100 Mbps full-duplex operation
- **100half** - Forces 100 Mbps half-duplex operation

- **10full** - Forces 10 Mbps full-duplex operation
- **10half** - Forces 10 Mbps half-duplex operation

Default Setting

- Auto-negotiation is enabled by default.
- When auto-negotiation is disabled, the default speed-duplex setting is 100half for 100BASE-TX ports and 1000full for Gigabit Ethernet ports.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- To force operation to the speed and duplex mode specified in a **speed-duplex** command, use the **no negotiation** command to disable auto-negotiation on the selected interface.
- When using the **negotiation** command to enable auto-negotiation, the optimal settings will be determined by the **capabilities** command. To set the speed/duplex mode under auto-negotiation, the required mode must be specified in the capabilities list for an interface.

Example

The following example configures port 5 to 100 Mbps, half-duplex operation.

```
Console(config)#interface ethernet 1/5
Console(config-if)#speed-duplex 100half
Console(config-if)#no negotiation
Console(config-if)#
```

Related Commands

negotiation (3-92)
capabilities (3-93)

negotiation

Use this command to enable autonegotiation for a given interface.
Use the **no** form to disable autonegotiation.

Syntax

negotiation
no negotiation

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- When auto-negotiation is enabled the switch will negotiate the best settings for a link based on the **capabilities** command. When auto-negotiation is disabled, you must manually specify the link attributes with the **speed-duplex** and **flowcontrol** commands.
- If autonegotiation is disabled, auto-MDI/MDI-X pin signal configuration will also be disabled for the RJ-45 ports.

Example

The following example configures port 11 to use autonegotiation.

```
Console(config)#interface ethernet 1/11
Console(config-if)#negotiation
Console(config-if)#
```

Related Commands

capabilities (3-93)
speed-duplex (3-90)
negotiation (3-92)

capabilities

Use this command to advertise the port capabilities of a given interface during autonegotiation. Use the **no** form with parameters to remove an advertised capability, or the **no** form without parameters to restore the default values.

Syntax

capabilities {**1000full** | **100full** | **100half** | **10full** | **10half** | **flowcontrol** | **symmetric**}

no port-capabilities [**1000full** | **100full** | **100half** | **10full** | **10half** | **flowcontrol** | **symmetric**]

- **1000full** - Supports 1000 Mbps full-duplex operation
- **100full** - Supports 100 Mbps full-duplex operation
- **100half** - Supports 100 Mbps half-duplex operation
- **10full** - Supports 10 Mbps full-duplex operation
- **10half** - Supports 10 Mbps half-duplex operation
- **flowcontrol** - Supports flow control
- **symmetric** (Gigabit only) - When specified, the port transmits and receives pause frames; when not specified, the port will auto-negotiate to determine the sender and receiver for asymmetric pause frames. (*The current switch ASIC only supports symmetric pause frames.*)

Default Setting

- Fast Ethernet: 10half, 10full, 100half, 100full
- Gigabit Ethernet: 1000full

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

When auto-negotiation is enabled with the **negotiation** command, the switch will negotiate the best settings for a link based on the **capabilities** command. When auto-negotiation is disabled, you must manually specify the link attributes with the **speed-duplex** and **flowcontrol** commands.

Example

The following example configures Ethernet port 5 capabilities to 100half, 100full and flow control.

```
Console(config)#interface ethernet 1/5
Console(config-if)#capabilities 100half
Console(config-if)#capabilities 100full
Console(config-if)#capabilities flowcontrol
Console(config-if)#
```

Related Commands

- negotiation (3-92)
- speed-duplex (3-90)
- flowcontrol (3-94)

flowcontrol

Use this command to enable flow control. Use the **no** form to disable flow control.

Syntax

- flowcontrol**
- no flowcontrol**

Default Setting

Flow control enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Flow control can eliminate frame loss by “blocking” traffic from end stations or segments connected directly to the switch when its buffers fill. When enabled, back pressure is used for half-duplex operation and IEEE 802.3x for full-duplex operation.
- To force flow control on or off (with the **flowcontrol** or **no flowcontrol** command), use the **no negotiation** command to disable auto-negotiation on the selected interface.
- When using the **negotiation** command to enable auto-negotiation, the optimal settings will be determined by the **capabilities** command. To enable flow control under auto-negotiation, “flowcontrol” must be included in the capabilities list for any port
- Avoid using flow control on a port connected to a hub unless it is actually required to solve a problem. Otherwise back pressure jamming signals may degrade overall performance for the segment attached to the hub.

Example

The following example enables flow control on port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#flowcontrol
Console(config-if)#no negotiation
Console(config-if)#
```

Related Commands

negotiation (3-92)

capabilities (flowcontrol, symmetric) (3-93)

shutdown

Use this command to disable an interface. To restart a disabled interface, use the **no** form.

Syntax

```
shutdown  
no shutdown
```

Default Setting

All interfaces are enabled.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This command allows you to disable a port due to abnormal behavior (e.g., excessive collisions), and then reenable it after the problem has been resolved. You may also want to disable a port for security reasons.

Example

The following example disables port 5.

```
Console(config)#interface ethernet 1/5  
Console(config-if)#shutdown  
Console(config-if)#
```

switchport broadcast percent

Use this command to configure broadcast storm control. Use the **no** form to disable broadcast storm control.

Syntax

switchport broadcast percent *level*
no switchport broadcast

level - Threshold level as a percentage of bandwidth.
(Range: 6 or 20 percent)

Default Setting

Enabled for all ports
Six percent of bandwidth

Command Mode

Interface Configuration (Ethernet)

Command Usage

- When broadcast traffic exceeds the specified threshold, packets above that threshold are dropped.
- This command can enable or disable broadcast storm control for the selected interface.

Example

The following shows how to configure broadcast storm control at 20% on port 3:

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport broadcast percent 20
Console(config-if)#
```

clear counters

Use this command to clear statistics on an interface.

Syntax

clear counters *interface*

interface

- **ethernet** *unit/port*
 - *unit* - This is device 1.
 - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-4)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Statistics are only initialized for a power reset. This command sets the base value for displayed statistics to zero for the current management session. However, if you log out and back into the management interface, the statistics displayed will show the absolute value accumulated since the last power reset.

Example

The following example clears statistics on Ethernet port 5.

```
Console#clear counters ethernet 1/5
Console#
```


show interfaces status

Use this command to display the status for an interface.

Syntax

show interfaces status *interface*

interface

- **ethernet** *unit/port*
 - *unit* - This is device 1.
 - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-4)
- **vlan** *vlan-id* (Range: 1-4094)

Default Setting

Shows status for all interfaces.

Command Mode

Normal Exec, Privileged Exec

Command Usage

If no interface is specified, information on all interfaces is displayed. For a description of the items displayed by this command, see “Displaying Connection Status” on page 2-30.

Example

```
Console#show interfaces status ethernet 1/3
Information of Eth 1/3
Basic information:
  Port type: 100TX
  Mac address: 00-55-FF-FF-DD-E0
Configuration:
  Name:
  Port admin: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full,
  Broadcast storm: Enabled
  Broadcast storm limit: 6 percent
  Flow control: Disabled
Current status:
  Link status: Down
  Operation speed-duplex: 10half
  Flow control type: None
Console#
```

show interfaces counters

Use this command to display statistics for an interface.

Syntax

show interfaces counters *interface*

interface

- **ethernet** *unit/port*
 - *unit* - This is device 1.
 - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-4)

Default Setting

Shows counters for all interfaces.

Command Mode

Normal Exec, Privileged Exec

Command Usage

If no interface is specified, information on all interfaces is displayed. For a description of the items displayed by this command, see “Showing Port Statistics” on page -96.

Example

```
Console#show interfaces counters ethernet 1/7
Ethernet 1/ 7
  Iftable stats:
    Octets input: 30658, Octets output: 196550
    Unicast input: 6, Unicast output: 5
    Discard input: 0, Discard output: 0
    Error input: 0, Error output: 0
    Unknown protos input: 0, QLen output: 0
  Extended iftable stats:
    Multi-cast input: 0, Multi-cast output: 3064
    Broadcast input: 262, Broadcast output: 1
  Ether-like stats:
    Alignment errors: 0, FCS errors: 0
    Single Collision frames: 0, Multiple collision frames: 0
    SQE Test errors: 0, Deferred transmissions: 0
    Late collisions: 0, Excessive collisions: 0
    Internal mac transmit errors: 0, Internal mac receive errors: 0
    Frame too longs: 0, Carrier sense errors: 0
    Symbol errors: 0
  RMON stats:
    Drop events: 0, Octets: 227208, Packets: 3338
    Broadcast pkts: 263, Multi-cast pkts: 3064
    Undersize pkts: 0, Oversize pkts: 0
    Fragments: 0, Jabbers: 0
    CRC align errors: 0, Collisions: 0
    Packet size <= 64 octets: 3150, Packet size 65 to 127 octets: 139
    Packet size 128 to 255 octets: 49, Packet size 256 to 511 octets: 0
    Packet size 512 to 1023 octets: 0, Packet size 1024 to 1518 octets: 0
Console#
```

show interfaces switchport

Use this command to display advanced interface configuration settings.

Syntax

show interfaces switchport [*interface*]

interface

- **ethernet** *unit/port*
 - *unit* - This is device 1.
 - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-4)

Default Setting

Shows all interfaces.

Command Mode

Normal Exec, Privileged Exec

Command Usage

If no interface is specified, information on all interfaces is displayed. The items displayed by this command include:

- **Broadcast threshold** – Shows if broadcast storm suppression is enabled or disabled; if enabled it also shows the threshold level (page 3-97).
- **VLAN membership mode** – Indicates membership mode as Trunk or Hybrid (page 3-125).
- **Ingress rule** – Shows if ingress filtering is enabled or disabled (page 3-127).
- **Acceptable frame type** – Shows if acceptable VLAN frames include all types or tagged frames only (page 3-126).
- **Native VLAN** – Indicates the default Port VLAN ID (page 3-128).
- **Priority for untagged traffic** – Indicates the default priority for untagged frames (page 3-146).

- **Gvrp status** – Shows if GARP VLAN Registration Protocol is enabled or disabled (page 3-140).
- **Allowed Vlan** – Shows the VLANs this interface has joined, where “(u)” indicates untagged and “(t)” indicates tagged (page 3-129).
- **Forbidden Vlan** – Shows the VLANs this interface can not dynamically join via GVRP (page 3-130).
- **Private-vlan mode** – Indicates if this interface is set to host mode or promiscuous mode (page 3-136).
- **Private-vlan host-association** – If this interface is set to host mode, this field shows the associated primary and secondary VLANs (page 3-137).
- **Private-vlan mapping** – If this interface is set to promiscuous mode, this field shows the primary VLAN and accessible secondary VLANs (page 3-138).

Example

This example shows the configuration for port 2 when set to host mode for private VLANs.

```

Console#show interfaces switchport ethernet 1/2
Information of Eth 1/2
Broadcast threshold: Enabled, 6 percent
VLAN membership mode: Access
Ingress rule: Enabled
Acceptable frame type: All frames
Native VLAN: 3
Priority for untagged traffic: 0
Gvrp status: Disabled
Allowed Vlan:      2(u),      3(u),
Forbidden Vlan:
Private-vlan mode: Host
Private-vlan host-association: Primary_vlan_ID:      2,
                               Secondary_vlan_ID:      3
Private-vlan mapping: NONE
Console#

```

This example shows the configuration for port 3 when set to promiscuous mode for private VLANs.

```
Console#show interfaces switchport ethernet 1/3
Information of Eth 1/3
Broadcast threshold: Enabled, 6 percent
VLAN membership mode: Access
Ingress rule: Enabled
Acceptable frame type: All frames
Native VLAN: 2
Priority for untagged traffic: 0
Gvrp status: Disabled
Allowed Vlan:      2(u),      3(u),
Forbidden Vlan:
Private-vlan mode: Promiscuous
Private-vlan mapping: Primary_vlan_ID:      2,
                      Secondary_vlan_ID:      2,      3,
Console#
```

Rate Limit Commands

This function allows the network manager to control the maximum rate for traffic transmitted or received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the network. Traffic that falls within the rate limit is transmitted, while packets that exceed the acceptable amount of traffic are dropped.

Rate limiting can be applied to individual ports or trunks. When an interface is configured with this feature, the traffic rate will be monitored by the hardware to verify conformity. Non-conforming traffic is dropped, conforming traffic is forwarded without any changes.

| Command | Function | Mode | Page |
|------------|---|------|-------|
| rate-limit | Sets the rate limit for the specified interface | IC | 3-105 |

rate-limit

Use this command to set the rate limit. Use the **no** form to remove the rate limit.

Syntax

rate-limit {input | output} percent *percent*
no rate-limit input

- **input** - Sets the rate limit for inbound traffic.
- **output** - Sets the rate limit for outbound traffic
- *percent* - Sets the rate limit to predefined percentage of bandwidth:

| Option | Percentage (based on port type) | | |
|--------|---------------------------------|----------|-----------|
| | 10 Mbps | 100 Mbps | 1000 Mbps |
| 3 | 312K | 3.12M | 31.2M |
| 6 | 625K | 6.25M | 62.5M |
| 9 | 938K | 9.38M | 93.8M |
| 12 | 1.25M | 12.5M | 125M |
| 20 | 2M | 20M | 200M |
| 40 | 4M | 40M | 400M |
| 60 | 6M | 60M | 600M |
| 80 | 8M | 80M | 800M |

Default Setting

No limit

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

This example sets the rate limit for input and output traffic on port 2 to 312K when operating at 10 Mbps or 3.12 Mbps when operating at 100 Mbps.

```
Console(config)#
Console(config)#interface ethernet 1/2
Console(config-if)#rate-limit input percent 3
Console(config-if)#rate-limit output percent 3
Console(config)#
```

Address Table Commands

These commands are used to configure the address table for filtering specified addresses, displaying current entries, clearing the table, or setting the aging time.

| Command | Function | Mode | Page |
|-----------------------------------|--|------|-------|
| mac-address-table static | Maps a static address to a port in a VLAN | GC | 3-107 |
| clear mac-address-table dynamic | Removes any learned entries from the forwarding database | PE | 3-108 |
| show mac-address-table | Displays entries in the bridge-forwarding database | PE | 3-109 |
| mac-address-table aging-time | Sets the aging time of the address table | GC | 3-110 |
| show mac-address-table aging-time | Shows the aging time for the address table | PE | 3-111 |

mac-address-table static

Use this command to map a static address to a destination port.
Use the **no** form to remove an address.

Syntax

mac-address-table static *mac-address* {*interface* | **discard**}
[*action*]

no mac-address-table static *mac-address* [**discard**]

- *mac-address* - MAC address.
- *interface*
 - **ethernet** *unit/port*
 - *unit* - This is device 1.
 - *port* - Port number.
 - **port-channel** *channel-id* (Range: 1-4)
- **discard** - Discards all packets matching the destination address.
- *action* -
 - **delete-on-reset** - Assignment lasts until switch is reset.
 - **permanent** - Assignment is permanent.

Default Setting

No static addresses are defined. The default mode is **permanent**.

Command Mode

Global Configuration

Command Usage

The static address for a host device can be assigned to a specific port within a specific VLAN. Use this command to add static addresses to the MAC Address Table. Static addresses have the following characteristics:

- Static addresses will not be removed from the address table when a given interface link is down.
- Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on an interface, the address will be ignored and will not be written to the address table.
- A static address cannot be learned on another port until the address is removed with the **no** form of this command.

Example

```
Console(config)#mac-address-table static 00-e0-29-94-34-de  
interface ethernet 1/1 vlan 1 delete-on-reset  
Console(config)#
```

clear mac-address-table dynamic

Use this command to remove any learned entries from the forwarding database and to clear the transmit and receive counts for any static or system configured entries.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#clear mac-address-table dynamic  
Console#
```

show mac-address-table

Use this command to view classes of entries in the bridge-forwarding database.

Syntax

show mac-address-table [**address** *mac-address* [*mask*]]
[**interface** *interface*] [**vlan** *vlan-id*] [**sort** {**address** | **vlan** | **interface**}]

- *mac-address* - MAC address.
- *mask* - Bits to ignore in the address.
- *interface*
 - **ethernet** *unit/port*
 - *unit* - This is device 1.
 - *port* - Port number.
 - **port-channel** *channel-id* (Range: 1-4)
- *vlan-id* - VLAN ID (Range: 1-4094)
- **sort** - Sort by address, vlan or interface.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- The MAC Address Table contains the MAC addresses associated with each interface. Note that the Type field may include the following types:
 - Learned - dynamic address entries
 - Permanent - static entry
 - Delete-on-reset - static entry to be deleted when system is reset
- The maximum number of address entries is 8191.

Example

```
Console#show mac-address-table
Interface Mac Address      Vlan Type
-----
Eth 1/ 1 00-e0-29-94-34-de 1 Delete-on-reset
Console#
```

mac-address-table aging-time

Use this command to set the aging time for entries in the address table. Use the **no** form to restore the default aging time.

Syntax

mac-address-table aging-time *seconds*
no mac-address-table aging-time

seconds - Time in seconds (2-172800).

Default Setting

300 seconds

Command Mode

Global Configuration

Command Usage

The aging time is used to age out dynamically learned forwarding information.

Example

```
Console(config)#mac-address-table aging-time 100
Console(config)#
```

show mac-address-table aging-time

Use this command to show the aging time for entries in the address table.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show mac-address-table aging-time
Aging time: 300 sec.
Console#
```

Spanning Tree Commands

This section includes commands that configure the Spanning Tree Algorithm (STA) globally for the switch, and commands that configure STA for the selected interface.

| Command | Function | Mode | Page |
|-----------------------------|--|------|-------|
| spanning-tree | Enables the spanning tree protocol | GC | 3-112 |
| spanning-tree forward-time | Configures the spanning tree bridge forward time | GC | 3-113 |
| spanning-tree hello-time | Configures the spanning tree bridge hello time | GC | 3-114 |
| spanning-tree max-age | Configures the spanning tree bridge maximum age | GC | 3-115 |
| spanning-tree priority | Configures the spanning tree bridge priority | GC | 3-116 |
| spanning-tree cost | Configures the spanning tree path cost of an interface | IC | 3-116 |
| spanning-tree port-priority | Configures the spanning tree priority of an interface | IC | 3-117 |

| Command | Function | Mode | Page |
|------------------------|--|------|-------|
| spanning-tree portfast | Sets an interface to fast forwarding | IC | 3-118 |
| show spanning-tree | Shows spanning tree configuration for the overall bridge or a selected interface | PE | 3-119 |

spanning-tree

Use this command to enable the Spanning Tree Algorithm globally for the switch. Use the **no** form to disable it.

Syntax

spanning-tree
no spanning-tree

Default Setting

Spanning tree is enabled.

Command Mode

Global Configuration

Command Usage

The Spanning Tree Algorithm (STA) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STA-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

Example

The following example shows how to enable the Spanning Tree Algorithm for the switch:

```
Console(config)#spanning-tree
Console(config)#
```

spanning-tree forward-time

Use this command to configure the spanning tree bridge forward time globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree forward-time *seconds*

no spanning-tree forward-time

seconds - Time in seconds. (Range: 4 - 30 seconds)

The minimum value is the higher of 4 or

$[(\text{max-age} / 2) + 1]$.

Default Setting

15 seconds

Command Mode

Global Configuration

Command Usage

This command sets the maximum time (in seconds) the root device will wait before changing states (i.e., listening to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result.

Example

```
Console(config)#spanning-tree forward-time 20
Console(config)#
```

spanning-tree hello-time

Use this command to configure the spanning tree bridge hello time globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree hello-time *time*

no spanning-tree hello-time

time - Time in seconds. (Range: 1-10 seconds).

The maximum value is the lower of 10 or $[(\text{max-age} / 2) - 1]$.

Default Setting

2 seconds

Command Mode

Global Configuration

Command Usage

This command sets the time interval (in seconds) at which the root device transmits a configuration message.

Example

```
Console(config)#spanning-tree hello-time 5
Console(config)#
```


spanning-tree max-age

Use this command to configure the spanning tree bridge maximum age globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree max-age *seconds*

no spanning-tree max-age

seconds - Time in seconds. (Range: 6-40 seconds)

The minimum value is the higher of 6 or
[2 x (hello-time + 1)].

The maximum value is the lower of 40 or
[2 x (forward-time - 1)].

Default Setting

20 seconds

Command Mode

Global Configuration

Command Usage

This command sets the maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network.

Example

```
Console(config)#spanning-tree max-age 40
Console(config)#
```

spanning-tree priority

Use this command to configure the spanning tree priority globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree priority *priority*
no spanning-tree priority

priority - Priority of the bridge. (Range: 0 - 65535)

Default Setting

32768

Command Mode

Global Configuration

Command Usage

Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.

Example

```
Console(config)#spanning-tree priority 40000
Console(config)#
```

spanning-tree cost

Use this command to configure the spanning tree path cost for the specified interface. Use the **no** form to restore the default.

Syntax

spanning-tree cost *cost*
no spanning-tree cost *cost*

cost - The path cost for the port. (Range: 1-65535)

The recommended range is:

- Ethernet: 50-600
- Fast Ethernet: 10-60
- Gigabit Ethernet: 3-10

Default Setting

- Ethernet – half duplex: 100; full duplex: 95; trunk: 90
- Fast Ethernet – half duplex: 19; full duplex: 18; trunk: 15
- Gigabit Ethernet – full duplex: 4; trunk: 3

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command is used by the spanning-tree algorithm to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media.
- Path cost takes precedence over port priority.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree cost 50
Console(config-if)#
```

spanning-tree port-priority

Use this command to configure the priority for the specified interface. Use the **no** form to restore the default.

Syntax

spanning-tree port-priority *priority*

no spanning-tree port-priority

priority - The priority for a port. (Range: 0-255)

Default Setting

128

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command defines the priority for the use of a port in the spanning-tree algorithm. If the path cost for all ports on a switch are the same, the port with the highest priority (that is, lowest value) will be configured as an active link in the spanning tree.
- Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree port-priority 0
Console(config-if)#
```

Related Commands

spanning-tree cost (3-116)

spanning-tree portfast

Use this command to set an interface to fast forwarding. Use the **no** form to disable fast forwarding.

Syntax

spanning-tree portfast
no spanning-tree portfast

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command is used to enable/disable the fast spanning-tree mode for the selected port. In this mode, ports skip the Blocked, Listening and Learning states and proceed straight to Forwarding.
- Since end-nodes cannot cause forwarding loops, they can be passed through the spanning tree state changes more quickly than allowed by standard convergence time. Fast forwarding can achieve quicker convergence for end-node workstations and servers, and also overcome other STA related timeout problems. (Remember that fast forwarding should only be enabled for ports connected to an end-node device.)

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree portfast
Console(config-if)#
```

show spanning-tree

Use this command to show the spanning tree configuration.

Syntax

show spanning-tree [*interface*]

interface

- **ethernet** *unit/port*
 - *unit* - This is device 1.
 - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-4)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

For a description of the items displayed under “Bridge-group information, see “Managing Global Settings” on page -43. For a description of the items displayed for specific interfaces, see “Managing STA Interface Settings” on page -47.

Example

```
Console#show spanning-tree ethernet 1/11
Bridge-group information
-----
Spanning tree protocol           :ieee8021d
Spanning tree enable/disable    :enable
Priority                         :32768
Hello Time (sec.)               :2
Max Age (sec.)                  :20
Forward Delay (sec.)            :15
Designated Root                 :32768.0000e9000066
Current root                    :0
Current root cost                :0
Number of topology changes      :1
Last topology changes time (sec.):2167
Hold times (sec.)               :1
-----
Eth 1/11 information
-----
Admin status                    : enable
STA state                       : broken
Path cost                       : 18
Priority                         : 128
Designated cost                 : 0
Designated port                 : 128.11
Designated root                 : 40000.123412341234
Designated bridge               : 32768.0000e9000066
Fast forwarding                 : disable
Forward transitions              : 0
Console#
```

VLAN Commands

A VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment. This section describes commands used to create VLAN groups, add port members, specify how VLAN tagging is used, and enable automatic VLAN registration for the selected interface.

| Command | Function | Mode | Page |
|-----------------------------------|--|------|-------|
| <i>Edit VLAN Groups</i> | | | |
| vlan database | Enters VLAN database mode to add, change, and delete VLANs | GC | 3-122 |
| vlan | Configures a VLAN, including VID, name and state | VC | 3-123 |
| <i>Configure VLAN Interfaces</i> | | | |
| interface vlan | Enters interface configuration mode for a specified VLAN | IC | 3-124 |
| switchport mode | Configures VLAN membership mode for an interface | IC | 3-125 |
| switchport acceptable-frame-types | Configures frame types to be accepted by an interface | IC | 3-126 |
| switchport ingress-filtering | Enables ingress filtering on an interface | IC | 3-127 |
| switchport native vlan | Configures the PVID (native VLAN) of an interface | IC | 3-128 |
| switchport allowed vlan | Configures the VLANs associated with an interface | IC | 3-129 |
| switchport gvrp | Enables GVRP for an interface | IC | 3-140 |
| switchport forbidden vlan | Configures forbidden VLANs for an interface | IC | 3-130 |

| Command | Function | Mode | Page |
|---------------------------------|---|-----------|-------|
| <i>Display VLAN Information</i> | | | |
| show vlan | Shows VLAN information | NE, PE | 3-131 |
| show interfaces status vlan | Displays status for the specified VLAN interface | NE, PE | 3-99 |
| show interfaces switchport | Displays the administrative and operational status of an interface | NE, PE | 3-102 |

vlan database

Use this command to enter VLAN database mode. All commands in this mode will take effect immediately.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- Use the VLAN database command mode to add, change, and delete VLANs. After finishing configuration changes, you can display the VLAN settings by entering the **show vlan** command.
- Use the **interface vlan** command mode to define the port membership mode and add or remove ports from a VLAN. The results of these commands are written to the running-configuration file, and you can display this file by entering the **show running-config** command.

Example

```
Console(config)#vlan database
Console(config-vlan)#
```


Related Commands

show vlan (3-131)

vlan

Use this command to configure a VLAN. Use the **no** form to restore the default settings or delete a VLAN.

Syntax

vlan *vlan-id* [**name** *vlan-name*] **media ethernet** [**state** {**active** | **suspend**}]

no vlan *vlan-id* [**name** | **state**]

- *vlan-id* - ID of configured VLAN. (Range: 1-4094, no leading zeroes)
- **name** - Keyword to be followed by the VLAN name.
 - *vlan-name* - ASCII string from 1 to 31 characters.
- **media ethernet** - Ethernet media type.
 - **state** - Keyword to be followed by the VLAN state.
 - **active** - VLAN is operational.
 - **suspend** - VLAN is suspended. Suspended VLANs do not pass packets.

Default Setting

By default only VLAN 1 exists and is active.

Command Mode

VLAN Database Configuration

Command Usage

- **no vlan** *vlan-id* deletes the VLAN.
- **no vlan** *vlan-id* **name** removes the VLAN name.
- **no vlan** *vlan-id* **state** returns the VLAN to the default state (i.e., active).

- VLAN 1 cannot be suspended, but any other VLAN will be suspended.
- You can configure up to 127 VLANs on the switch.

Example

The following example adds a VLAN, using vlan-id 105 and name RD5. The VLAN is activated by default.

```
Console(config)#vlan database
Console(config-vlan)#vlan 105 name RD5 media ethernet
Console(config-vlan)#
```

Related Commands

show vlan (3-131)

interface vlan

Use this command to enter interface configuration mode for VLANs, and configure a physical interface.

Syntax

interface vlan *vlan-id*

vlan-id - ID of the configured VLAN. (Range: 1-4094, no leading zeroes)

Default Setting

None

Command Mode

Global Configuration

Example

The following example shows how to set the interface configuration mode to VLAN 1, and then assign an IP address to the VLAN:

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.254 255.255.255.0
Console(config-if)#
```

Related Commands

shutdown (3-96)

switchport mode

Use this command to configure the VLAN membership mode for a port. Use the **no** form to restore the default.

Syntax

switchport mode {trunk | access}

no switchport mode

- **trunk** - Specifies a port as an end-point for a VLAN trunk. A trunk is a direct link between two switches, so the port transmits tagged frames that identify the source VLAN. However, note that frames belonging to the port's default VLAN (i.e., associated with the PVID) are sent untagged.
- **access** - Sets the port to operate as an untagged interface. All frames are sent untagged.

Default Setting

All ports are in access mode with the PVID set to VLAN 1.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

The following shows how to set the configuration mode to port 1, and then set the switchport mode to trunk:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport mode trunk
Console(config-if)#
```

switchport acceptable-frame-types

Use this command to configure the acceptable frame types for a port. Use the **no** form to restore the default.

Syntax

switchport acceptable-frame-types {all | tagged}
no switchport acceptable-frame-types

- **all** - The port accepts all frames, tagged or untagged.
- **tagged** - The port only receives tagged frames.

Default Setting

All frame types

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

When set to receive all frame types, any received frames that are untagged are assigned to the default VLAN.

Example

The following example shows how to restrict the traffic received on port 1 to tagged frames:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#
```

switchport ingress-filtering

Use this command to enable ingress filtering for an interface. Use the **no** form to restore the default.

Syntax

switchport ingress-filtering
no switchport ingress-filtering

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Ingress filtering only affects tagged frames.
- If ingress filtering is disabled, the interface will accept any VLAN-tagged frame if the tag matches a VLAN known to the switch (except for VLANs explicitly forbidden on this port).
- If ingress filtering is enabled, incoming frames tagged for VLANs which do not include this ingress port in their member set will be discarded.
- Ingress filtering does not affect VLAN independent BPDU frames, such as GVRP or STA. However, they do affect VLAN dependent BPDU frames, such as GMRP.

Example

The following example shows how to set the interface to port 1 and then enable ingress filtering:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport ingress-filtering
Console(config-if)#
```

switchport native vlan

Use this command to configure the PVID (i.e., default VLAN ID) for a port. Use the **no** form to restore the default.

Syntax

switchport native vlan *vlan-id*
no switchport native vlan

vlan-id - Default VLAN ID for a port. (Range: 1-4094, no leading zeroes)

Default Setting

VLAN 1

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- If an interface is not a member of VLAN 1 and you assign its PVID to this VLAN, the interface will automatically be added to VLAN 1 as an untagged member. For all other VLANs, an interface must first be configured as an untagged member before you can assign its PVID to that group.
- If acceptable frame types is set to **all** or switchport mode is set to **hybrid**, the PVID will be inserted into all untagged frames entering the ingress port.

Example

The following example shows how to set the PVID for port 1 to VLAN 3:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport native vlan 3
Console(config-if)#
```

switchport allowed vlan

Use this command to configure VLAN groups on the selected interface. Use the **no** form to restore the default.

Syntax

switchport allowed vlan {add *vlan* | remove *vlan*}
no switchport allowed vlan

- **add *vlan*** - VLAN identifier to add.
- **remove *vlan*** - VLAN identifier to remove.

Do not enter leading zeros. (Range: 1-4094)

Default Setting

All ports are assigned to VLAN 1 by default.
The default frame type is untagged.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- If switchport mode is set to **trunk**, then you can only assign an interface to VLAN groups as a tagged member.
- Frames are always tagged within the switch. The tagged/untagged parameter used when adding a VLAN to an interface tells the switch whether to keep or remove the tag from a frame on egress.
- If none of the intermediate network devices nor the host at the other end of the connection supports VLANs, the interface should be added to these VLANs as an untagged member. Otherwise, it is only necessary to add at most one VLAN as untagged, and this should correspond to the native VLAN for the interface.
- If a VLAN on the forbidden list for an interface is manually added to that interface, the VLAN is automatically removed from the forbidden list for that interface.

Example

The following example shows how to add VLANs 1, 2, 5 and 6 to the allowed list as tagged VLANs for port 1:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport allowed vlan add 1
Console(config-if)#switchport allowed vlan add 2
Console(config-if)#switchport allowed vlan add 5
Console(config-if)#switchport allowed vlan add 6
Console(config-if)#
```

switchport forbidden vlan

Use this command to configure forbidden VLANs. Use the **no** form to remove the list of forbidden VLANs.

Syntax

switchport forbidden vlan {add *vlan* | remove *vlan*}
no switchport forbidden vlan

- **add *vlan*** - VLAN ID to add.
- **remove *vlan*** - VLAN ID to remove.

Do not enter leading zeroes. (Range: 1-4094)

Default Setting

No VLANs are included in the forbidden list.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command prevents a VLAN from being automatically added to the specified interface via GVRP.
- If a VLAN has been added to the set of allowed VLANs for an interface, then you cannot add it to the set of forbidden VLANs for that same interface.

Example

The following example shows how to prevent port 1 from being added to VLAN 3:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport forbidden vlan add 3
Console(config-if)#
```

show vlan

Use this command to show VLAN information.

Syntax

show vlan [**id** *vlan-id* | **name** *vlan-name*]

- **id** - Keyword to be followed by the VLAN ID.
 - *vlan-id* - ID of the configured VLAN. (Range: 1-4094, no leading zeroes)
- **name** - Keyword to be followed by the VLAN name.
 - *vlan-name* - ASCII string from 1 to 32 characters.

Default Setting

Shows all VLANs.

Command Mode

Normal Exec, Privileged Exec

Example

The following example shows how to display information for VLAN 1:

| | | | | | | | | |
|------------------------|--------|-------------|--------|----------------------|---------|---------|---------|--|
| Console#show vlan id 1 | | | | | | | | |
| VLAN | Type | Name | Status | Ports/Channel groups | | | | |
| ----- | | | | | | | | |
| 1 | Static | DefaultVlan | Active | Eth1/1 | Eth1/2 | Eth1/3 | Eth1/4 | |
| | | | | Eth1/5 | Eth1/6 | Eth1/7 | Eth1/8 | |
| | | | | Eth1/9 | Eth1/10 | Eth1/11 | Eth1/12 | |
| | | | | Eth1/13 | Eth1/14 | Eth1/15 | Eth1/16 | |
| | | | | Eth1/17 | Eth1/18 | Eth1/19 | Eth1/20 | |
| | | | | Eth1/21 | Eth1/22 | Eth1/23 | Eth1/24 | |
| Console# | | | | | | | | |

Private VLAN Commands

Private VLANs provide port-based security and isolation between ports within the assigned VLAN. This switch supports two types of private VLAN ports: promiscuous, and community ports. A promiscuous port can communicate with all interfaces within a private VLAN. Community ports can only communicate with other ports in their own community VLAN, and with their designated promiscuous ports. This section describes commands used to configure private VLANs.

| Command | Function | Mode | Page |
|--|--|------|-------|
| <i>Edit Private VLAN Groups</i> | | | |
| private-vlan | Adds or deletes primary and secondary VLANs | VC | 3-134 |
| private-vlan association | Associates a secondary with a primary VLAN | VC | 3-135 |
| <i>Configure Private VLAN Interfaces</i> | | | |
| switchport mode private-vlan | Sets an interface to host mode or promiscuous mode | IC | 3-136 |

| Command | Function | Mode | Page |
|--|---|-----------|-------|
| switchport private-vlan host-association | Associates an interface with a secondary VLAN | IC | 3-137 |
| switchport private-vlan mapping | Maps an interface to a primary VLAN | IC | 3-138 |
| Display Private VLAN Information | | | |
| show vlan private-vlan | Shows private VLAN information | NE, PE | 3-139 |

To configure private VLANs, follow these steps:

1. Use the **private-vlan** command to designate one or more community VLANs and the primary VLAN that will channel traffic outside the community groups.
2. Use the **private-vlan association** command to map the secondary (i.e., community) VLAN(s) to the primary VLAN.
3. Use the **switchport mode private-vlan** command to configure ports as promiscuous (i.e., having access to all ports in the primary VLAN) or host (i.e., having access restricted to community VLAN members, and channeling all other traffic through a promiscuous port).
4. Use the **switchport private-vlan host-association** command to assign a port to a secondary VLAN.
5. Use the **switchport private-vlan mapping** command to assign a port to a primary VLAN.
6. Use the **show vlan private-vlan** command to verify your configuration settings.

private-vlan

Use this command to create a primary or secondary (i.e., community) private VLAN. Use the **no** form to remove the specified private VLAN.

Syntax

private-vlan *vlan-id* {**community** | **primary**}

no private-vlan *vlan-id*

- *vlan-id* - ID of private VLAN. (Range: 2-4094, no leading zeroes).
- **community** - A VLAN in which traffic is restricted to port members.
- **primary** - A VLAN which can contain one or more community VLANs, and serves to channel traffic between community VLANs and other locations.

Default Setting

None

Command Mode

VLAN Configuration

Command Usage

- Private VLANs are used to restrict traffic to ports within the same VLAN “community,” and channel traffic passing outside the community through promiscuous ports that have been mapped to the associated “primary” VLAN.
- Port membership for private VLANs is static. Once a port has been assigned to a private VLAN, it cannot be dynamically moved to another VLAN via GVRP.
- Private VLAN ports cannot be set to trunked mode. (See “switchport mode” on page 125.)

Example

```
Console(config)#vlan database
Console(config-vlan)#private-vlan 2 primary
Console(config-vlan)#private-vlan 3 community
Console(config)#
```

private vlan association

Use this command to associate a primary VLAN with a secondary (i.e., community) VLAN. Use the **no** form to remove all associations for the specified primary VLAN.

Syntax

private-vlan *primary-vlan-id* **association** [*secondary-vlan-id* | **add** *secondary-vlan-id* | **remove** *secondary-vlan-id*]

no private-vlan *primary-vlan-id* **association**

- *primary-vlan-id* - ID of primary VLAN.
(Range: 2-4094, no leading zeroes).
- *secondary-vlan-id* - ID of secondary (i.e., community) VLAN.
(Range: 2-4094, no leading zeroes).

Default Setting

None

Command Mode

VLAN Configuration

Command Usage

Secondary VLANs provide security for group members. The associated primary VLAN provides a common interface for access to other network resources within the primary VLAN (e.g., servers configured with promiscuous ports) and to resources outside of the primary VLAN (via promiscuous ports).

Example

```
Console(config-vlan)#private-vlan 2 association 3
Console(config)#
```

switchport mode private-vlan

Use this command to set the private VLAN mode for an interface.
Use the **no** form to restore the default setting.

Syntax

switchport mode private-vlan {host | promiscuous}
no switchport mode private-vlan

- **host** - This port type can communicate with all other host ports assigned to the same secondary VLAN. All communications outside of this VLAN must pass through a promiscuous port in the associated primary VLAN.
- **promiscuous** - This port type can communicate with all other promiscuous ports in the same primary VLAN, as well as with all the ports in the associated secondary VLANs.

Default Setting

Normal VLAN

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

Promiscuous ports assigned to a primary VLAN can communicate with all other promiscuous ports in the same VLAN, as well as with all the ports in the associated secondary VLANs.

Example

```
Console(config)#interface ethernet 1/2
Console(config-if)#switchport mode private-vlan promiscuous
Console(config)#exit
Console(config)#interface ethernet 1/3
Console(config-if)#switchport mode private-vlan host
Console(config)#
```

switchport private-vlan host-association

Use this command to associate an interface with a secondary VLAN. Use the **no** form to remove this association.

Syntax

switchport private-vlan host-association *secondary-vlan-id*
no switchport private-vlan host-association

secondary-vlan-id - ID of secondary (i.e, community) VLAN.
(Range: 2-4094, no leading zeroes).

Default Setting

None

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

All ports assigned to a secondary (i.e., community) VLAN can pass traffic between group members, but must communicate with resources outside of the group via a promiscuous port.

Example

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport private-vlan host-association 3
Console(config)#
```

switchport private-vlan mapping

Use this command to map an interface to a primary VLAN. Use the **no** form to remove this mapping.

Syntax

switchport private-vlan mapping *primary-vlan-id*
no switchport private-vlan mapping

primary-vlan-id - ID of primary VLAN. (Range: 2-4094, no leading zeroes).

Default Setting

None

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

Promiscuous ports assigned to a primary VLAN can communicate with any other promiscuous ports in the same VLAN, and with the group members within any associated secondary VLANs.

Example

```
Console(config)#interface ethernet 1/2
Console(config-if)#switchport private-vlan mapping 2
Console(config)#
```


show vlan private-vlan

Use this command to show the private VLAN configuration settings on this switch.

Syntax

show vlan private-vlan [**community** | **primary**]

- **community** - Displays all community VLANs, along with their associate primary VLAN and assigned host interfaces.
- **primary** - Displays all primary VLANs, along with any assigned promiscuous interfaces.

Default Setting

None

Command Mode

Privileged Exec

Example

```

Console#sh vlan private-vlan
Primary    Secondary    Type          Interfaces
-----
      2                primary      Eth1/ 2
      2             3    community    Eth1/ 3
      2             4    community    Eth1/ 4
      2             5    community    Eth1/ 5
      6                primary      Eth1/ 6
      6             7    community    Eth1/ 7
      6             8    community    Eth1/ 8
      6             9    community    Eth1/ 9
Console#

```

GVRP and Bridge Extension Commands

GARP VLAN Registration Protocol defines a way for switches to exchange VLAN information in order to automatically register VLAN members on interfaces across the network. This section describes how to enable GVRP for individual interfaces and globally for the switch, as well as how to display default configuration settings for the Bridge Extension MIB.

| Command | Function | Mode | Page |
|---------------------------|--|--------|-------|
| <i>Interface Commands</i> | | | |
| switchport gvrp | Enables GVRP for an interface | IC | 3-140 |
| switchport forbidden vlan | Configures forbidden VLANs for an interface | IC | 3-130 |
| show gvrp configuration | Displays GVRP configuration for selected interface | NE, PE | 3-141 |
| garp timer | Sets the GARP timer for the selected function | IC | 3-142 |
| show garp timer | Shows the GARP timer for the selected function | NE, PE | 3-143 |
| <i>Global Commands</i> | | | |
| bridge-ext gvrp | Enables GVRP globally for the switch | GC | 3-144 |
| show bridge-ext | Shows bridge extension configuration | PE | 3-145 |

switchport gvrp

Use this command to enable GVRP for a tagged port. Use the **no** form to disable it.

Syntax

switchport gvrp
no switchport gvrp

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

GVRP can only be enabled for tagged ports. You must set **switchport mode** to “trunk” to configure a tagged port.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport gvrp
Console(config-if)#
```

Related Commands

switchport mode (3-125)

show gvrp configuration

Use this command to show if GVRP is enabled.

Syntax

show gvrp configuration [*interface*]

interface

- **ethernet** *unit/port*
 - *unit* - This is device 1.
 - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-4)

Default Setting

Shows both global and interface-specific configuration.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show gvrp configuration ethernet 1/7
Eth 1/ 7:
  Gvrp configuration: Disabled
Console#
```

garp timer

Use this command to set the values for the join, leave and leaveall timers. Use the **no** form to restore the timers' default values.

Syntax

garp timer {join | leave | leaveall} timer_value
no garp timer {join | leave | leaveall}

- **{join | leave | leaveall}** - Which timer to set.
- **timer_value** - Value of timer.

Ranges:

join: 20-1000 centiseconds

leave: 60-3000 centiseconds

leaveall: 500-18000 centiseconds

Default Setting

- join: 20 centiseconds
- leave: 60 centiseconds
- leaveall: 1000 centiseconds

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Group Address Registration Protocol is used by GVRP and GMRP to register or deregister client attributes for client services within a bridged LAN. The default values for the GARP timers are independent of the media access method or data rate. These values should not be changed unless you are

experiencing difficulties with GMRP or GVRP registration/deregistration.

- Timer values are applied to GVRP for all the ports on all VLANs.
- Timer values must meet the following restrictions:
 - leave >= (2 x join)
 - leaveall > leave

Note: Set GVRP timers on all Layer 2 devices connected in the same network to the same values. Otherwise, GVRP will not operate successfully.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#garp timer join 100
Console(config-if)#
```

Related Commands

show garp timer (3-143)

show garp timer

Use this command to show the GARP timers for the selected interface.

Syntax

show garp timer [*interface*]

interface

- **ethernet** *unit/port*
 - *unit* - This is device 1.
 - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-4)

Default Setting

Shows all GARP timers.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show garp timer ethernet 1/1
Eth 1/ 1 GARP timer status:
  Join timer: 20 centiseconds
  Leave timer: 60 centiseconds
  Leaveall timer: 1000 centiseconds
Console#
```

Related Commands

garp timer (3-142)

bridge-ext gvrp

Use this command to enable GVRP. Use the **no** form to disable it.

Syntax

bridge-ext gvrp
no bridge-ext gvrp

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

GVRP defines a way for switches to exchange VLAN information in order to register VLAN members on ports across the network. This function should be enabled to permit automatic VLAN registration, and to support VLANs which extend beyond the local switch.

Example

```
Console(config)#bridge-ext gvrp
Console(config)#
```

show bridge-ext

Use this command to show the configuration for bridge extension commands.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

See “Displaying Basic VLAN Information” on page -56 and “Displaying Bridge Extension Capabilities” on page -24 for a description of the displayed items.

Example

```
Console#show bridge-ext
Max support vlan numbers: 127
Max support vlan ID: 4094
Extended multicast filtering services: No
Static entry individual port: Yes
VLAN learning: SVL
Configurable PVID tagging: Yes
Local VLAN capable: No
Traffic classes: Enabled
Global GVRP status: Disabled
GMRP: Disabled
Console#
```

Priority Commands

Class of Service (CoS) allows data packets that have greater precedence to receive higher service priority when traffic is buffered in the switch due to congestion. This switch supports CoS with four priority queues for each port. Data packets in a port's high-priority queues will be transmitted before those in the lower-priority queues.

You can set the switch to service the queues based on a strict rule that requires all traffic in a higher priority queue to be processed before lower priority queues are serviced, or use Weighted Round-Robin (WRR) queuing that specifies a relative weight of each queue. WRR uses a predefined relative weight for each queue that determines the percentage of service time the switch services each queue before moving on to the next queue. This prevents the head-of-line blocking that can occur with strict priority queuing.

Inbound frames that do not have VLAN tags are tagged with a default service priority of zero, and placed in queue 1 at the output port. Therefore, any inbound frames that do not have priority tags will be placed in queue 1 of the output port. (Note that if the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.) However, if the incoming frame is an IEEE 802.1Q VLAN tagged frame, the IEEE 802.1p User Priority bits will be used.

| Command | Function | Mode | Page |
|-----------------|--|-----------|-------|
| queue mode | Sets the queue mode to strict priority or Weighted Round-Robin (WRR) | GC | 3-147 |
| show queue mode | Shows the current queue mode | NE, PE | 3-147 |

queue mode

Use this command to set the queue mode to strict priority or Weighted Round-Robin (WRR) for the four class of service (CoS) priority queues. Use the **no** form to restore the default value.

Syntax

queue mode {strict | wrr}
no queue mode

- **strict** - Services the egress queues in sequential order, transmitting all traffic in the higher priority queues before servicing lower priority queues.
- **wrr** - Weighted Round-Robin shares bandwidth at the egress ports by using scheduling weights of 1, 3, 12 and 48 for queue 0, 1, 2 and 3 respectively.

Default Setting

Weighted Round Robin

Command Mode

Global Configuration

Example

The following example sets the queue mode to strict priority service mode:

```
Console(config)#queue mode strict
Console(config)#
```

show queue mode

Use this command to show the current queue mode.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#sh queue mode

Wrr status: Enabled
Console#
```

Mirror Port Commands

This section describes how to mirror traffic from a source port to a target port.

| Command | Function | Mode | Page |
|-------------------|---|------|-------|
| port monitor | Configures a mirror session | IC | 3-148 |
| show port monitor | Shows the configuration for a mirror port | PE | 3-149 |

port monitor

Use this command to configure a mirror session. Use the **no** form to clear a mirror session.

Syntax

port monitor *interface* [**rx** | **tx** | **both**]
no port monitor *interface*

- *interface* - **ethernet** *unit/port* (source port)
 - *unit* - Switch (unit 1).
 - *port* - Port number.
- **rx** - Mirror received packets.
- **tx** - Mirror transmitted packets.
- **both** - Mirror both received and transmitted packets.

Default Setting

No mirror session is defined. When enabled, the default mirroring is for both received and transmitted packets.

Command Mode

Interface Configuration (Ethernet, destination port)

Command Usage

- You can mirror traffic from any source port to a destination port for real-time analysis. You can then attach a logic analyzer or RMON probe to the destination port and study the traffic crossing the source port in a completely unobtrusive manner.
- The destination port is set by specifying an Ethernet interface.
- The mirror port and monitor port speeds must match, otherwise traffic may be dropped from the monitor port.
- You can create multiple mirror sessions, but all must share the same destination port. However, you should avoid sending too much traffic to the destination port from multiple source ports.

Example

The following example configures the switch to mirror all packets from port 6 to port 11:

```
Console(config)#interface ethernet 1/11
Console(config-if)#port monitor ethernet 1/6 both
Console(config-if)#
```

show port monitor

Use this command to display mirror information.

Syntax

show port monitor [*interface*]

interface - **ethernet** *unit/port* (source port)

- *unit* - Switch (unit 1).
- *port* - Port number.

Default Setting

Shows all sessions.

Command Mode

Privileged Exec

Command Usage

This command displays the currently configured source port, destination port, and mirror mode (i.e., RX, TX, RX/TX).

Example

The following shows mirroring configured from port 6 to port 11:

```
Console(config)#interface ethernet 1/11
Console(config-if)#port monitor ethernet 1/6
Console(config-if)#end
Console#show port monitor
Port Mirroring
-----
Destination port(listen port):Eth1/1
Source port(monitored port)  :Eth1/6
Mode                        :RX/TX
Console#
```

Port Trunking Commands

Ports can be statically grouped into an aggregate link (i.e., trunk) to increase the bandwidth of a network connection or to ensure fault recovery. You can configure trunks between switches of the same type. All switches have to comply with the Cisco EtherChannel standard. This switch supports up to four trunks. For example, a trunk consisting of two 1000 Mbps ports can support an aggregate bandwidth of 4 Gbps when operating at full duplex.

| Command | Function | Mode | Page |
|--|--|-------------|-------------|
| interface port-channel | Configures a trunk and enters interface configuration mode for the trunk | GC | 3-89 |
| port-group | Adds a predefined port group to a trunk | IC | 3-152 |
| show interfaces status port-channel | Shows trunk information | NE, PE | 3-99 |

Guidelines for Creating Trunks

- Finish configuring port trunks before you connect the corresponding network cables between switches to avoid creating a loop.
- A trunk can contain up to eight 10/100 Mbps ports or up to two 1000 Mbps ports.
- The ports at both ends of a connection must be configured as trunk ports.
- All ports in a trunk must consist of the same media type (i.e., twisted-pair or fiber).
- All ports in a trunk must be configured in an identical manner, including communication mode (i.e., speed, duplex mode and flow control), VLAN assignments, and CoS settings.
- All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN via the specified port-channel.
- STP, VLAN, and IGMP settings can only be made for the entire trunk via the specified port-channel.

port-group

Use this command to add a predefined port group to a trunk. Use the **no** form to remove a port group from a trunk.

Syntax

```
port-group port-group-number
no port-group
```

port-group-number - Group number (Range: 1-10)

| Group Number | Ports |
|--------------|-------------|
| 1 | 1, 13 |
| 2 | 1-2, 13-14 |
| 3 | 1-4, 13-16 |
| 4 | 5, 17 |
| 5 | 5-6, 17-18 |
| 6 | 5-8, 17-20 |
| 7 | 9, 21 |
| 8 | 9-10, 21-22 |
| 9 | 9-12, 21-24 |
| 10 | 25-26 |

Default Setting

None

Command Mode

Interface Configuration (Port Channel)

Command Usage

- Use **no channel-group** to remove a port group from a trunk.
- Use **no interfaces port-channel** to remove a trunk from the switch.

Example

The following example creates trunk 1 and then adds port 1 and 13:

```
Console(config)#interface port-channel 1
Console(config-if)#port-group 1
Console(config-if)#
```


APPENDIX A

TROUBLESHOOTING

Troubleshooting Chart

| Troubleshooting Chart | |
|--|---|
| Symptom | Action |
| Cannot connect using Telnet, Web browser, or SNMP software | <ul style="list-style-type: none">• Be sure to have configured the agent with a valid IP address, subnet mask and default gateway.• Be sure that your management station has access to management VLAN (default is VLAN 1).• Check that you have a valid network connection to the switch and that the port you are using has not been disabled.• Check network cabling between the management station and the switch.• If you cannot connect using Telnet, you may have exceeded the maximum number of concurrent Telnet sessions permitted. Try connecting again at a later time. |

| Troubleshooting Chart | |
|---|---|
| Symptom | Action |
| Cannot access the on-board configuration program via a serial port connection | <ul style="list-style-type: none">• Be sure to have set the terminal emulator program to VT100 compatible, 8 data bits, 1 stop bit, no parity and 9600 bps.• Check that the null-modem serial cable conforms to the pin-out connections provided in Appendix B. |
| Forgot or lost the password | <ul style="list-style-type: none">• Reinstall the switch defaults. Make a direct connection to the switch's console port and power cycle the switch. During the POST diagnostics, access the firmware-download menu and select the appropriate options. See "Restoring Switch Defaults" on page B-4 for more details. |

APPENDIX B

UPGRADING FIRMWARE VIA THE SERIAL PORT

The switch contains three firmware components that can be upgraded; the diagnostics (or Boot-ROM) code, runtime operation code and the loader code. The runtime code can be upgraded via the switch's RS-232 serial console port, via a network connection to a TFTP server, or using SNMP management software. The diagnostics and the loader code can be upgraded only via the switch's RS-232 serial console port.

Note: You can use the switch's Web interface to download runtime code via TFTP. Downloading large runtime code files via TFTP is normally much faster than downloading via the switch's serial port.

You can upgrade switch firmware by connecting a PC directly to the serial console port on the switch's front panel and using VT100 terminal emulation software that supports the XModem protocol. (See "Required Connections" on page 1-3.)

1. Connect a PC to the switch's console port using a null-modem or crossover RS-232 cable with a female DB-9 connector.
2. Configure the terminal emulation software's communication parameters to 9600 baud, 8 data bits, 1 stop bit, no parity, and set flow control to *none*.
3. Power cycle the switch.

4. When the switch initialization screen appears, enter firmware-download mode by pressing <Esc> immediately after the diagnostic test results. Screen text similar to that shown below displays:

```
[1]Image Update
[2]System Parameters
[3]Change Baud rate
[4]Do all the following Test
[5]Testing the System SDRAM
[6]MPC 850 internal clock Timer and Interrupt Test
[7]WATCHDOG Timer and Interrupt Test
[8]ACD chip Test
[9]Switch Loopback Test
[G]oto System
ReB[O]ot Again
Enter Selection:
```

5. Press <3> to change the baud rate of the switch's serial connection.

```
Enter Selection: 5
Change main console baudrate :
[0] Quit
[1] 9600 bps
[2] 19200 bps
[3] 38400 bps
[4] 57600 bps
[5] 115200 bps
```

6. There are five baud rate settings available, 9600, 19200, 38400, 57600 and 115200. Using the highest baud rate minimizes the time required to download firmware code files. Press <5> to select the option for 115200 baud.
7. Set your PC's terminal emulation software to match the 115200 baud rate. Press <Enter> to reset communications with the switch.
8. Press <1> to start to download the new code file.

9. If using Windows HyperTerminal, click the “Transfer” button, and then click “Send File....” Select the XModem Protocol and then use the “Browse” button to select the required firmware code file from your PC system. The “Xmodem file send” window displays the progress of the download procedure.
10. After the file has been downloaded, you are prompted with “Update Image File:” to specify the type of code file. Press <R> for runtime code, <D> for diagnostic code, or <L> for loader code.

Caution: If you select <L> for loader code, be sure the code is valid. Otherwise the switch will not be able to boot. Unless absolutely necessary do not download loader files.

11. Specify a name for the downloaded code file. Filenames should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names is 31 characters. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")
12. If you are downloading a runtime code file you must enter the same filename as the current runtime file to overwrite that file. The switch can only contain one runtime file.

For example, the following screen text shows the download procedure for a runtime code file:

```
Image download at Baudrate [115200]. Please Change your setting
Xmodem Receiving Start ::
Image downloaded to buffer.

        [R]untime
        [D]iagnostic
        [L]oader (Warning: you sure what you are doing?)
Update Image File:r
Runtime Image Filename : acd
Updating file system.
File system updated.
Please change your Baudrate to default then press any key to continue
```

13. Set your PC's terminal emulation software baud rate back to 9600 baud. Press <Enter> to reset communications with the switch.
14. Enter <G> to boot the system.

Restoring Switch Defaults

1. If you have lost your password for management access to the switch, you can load the default configuration file to restore the default passwords. When the switch initialization screen appears, enter firmware-download mode by pressing <ESC> immediately after the diagnostic test results. Press <Ctrl + G> followed by <Enter>. The following menu will appear:

```
Enter Selection:
[0]FileManager:
[1]Test Mode Set:
[x] Exit !
Enter Selection:0
```

2. Enter <0> to access the File Manager menu. The following screen will appear:

| File Name | S/Up | Type | Size |
|--|------|------|--------|
| Factory_Default_Config.cfg | 0 | 5 | 2536 |
| acd | 1 | 2 | 756608 |
| config1 | 1 | 5 | 3044 |
| diag_1005.bix | 1 | 1 | 78976 |
| ----- | | | |
| [X]modem Download [D]elete File [S]et Startup File | | | |
| [E]rase the whole flash [Q]uit | | | |
| Select> | | | |

3. Enter <S> and set the Factory_Default_config.cfg file as the startup configuration file.

| File name to set as default : Factory_Default_Config.cfg | | | |
|--|------|------|--------|
| File Type : [R]untime [D]iag [C]onfig > c | | | |
| File Name | S/Up | Type | Size |
| Factory_Default_Config.cfg | 1 | 5 | 2536 |
| acd | 1 | 2 | 756608 |
| config1 | 0 | 5 | 3044 |
| diag_1005.bix | 1 | 1 | 78976 |
| ----- | | | |
| [X]modem Download [D]elete File [S]et Startup File | | | |
| [E]rase the whole flash [Q]uit | | | |
| Select> | | | |

4. Enter <q> and then <x> to return to the main menu.

```
Select> q
[0]FileManager:
[1]Test Mode Set:
[x] Exit !
Enter Selection:x
```

```
[0]FileManager:
[1]Test Mode Set:
[x] Exit !
Enter Selection:x
[1]Image Update
[2]System Parameters
[3]Change Baud rate
[4]Do all the following Test
[5]Testing the System SDRAM
[6]MPC 850 internal clock Timer and Interrupt Test
[7]WATCHDOG Timer and Interrupt Test
[8]ACD chip Test
[9]Switch Loopback Test
[G]oto System
```

5. Enter <G> to boot the system.

GLOSSARY

10BASE-T

IEEE 802.3 specification for 10 Mbps Ethernet over two pairs of Category 3, 4, or 5 UTP cable.

100BASE-TX

IEEE 802.3u specification for 100 Mbps Fast Ethernet over two pairs of Category 5 UTP cable.

1000BASE-T

IEEE 802.3ab specification for Gigabit Ethernet over two pairs of Category 5, 5e 100-ohm UTP cable.

1000BASE-X

IEEE 802.3 shorthand term for any 1000 Mbps Gigabit Ethernet based on 8B/10B signaling.

Auto-negotiation

Signalling method allowing each node to select its optimum operational mode (e.g., 10 Mbps or 100 Mbps and half or full duplex) based on the capabilities of the node to which it is connected.

Bandwidth

The difference between the highest and lowest frequencies available for network signals. Also synonymous with wire speed, the actual speed of the data transmission along the cable.

BOOTP

Boot protocol used to load the operating system for devices connected to the network.

Collision

A condition in which packets transmitted over the cable interfere with each other. Their interference makes both signals unintelligible.

Collision Domain

Single CSMA/CD LAN segment.

CSMA/CD

Carrier Sense Multiple Access/Collision Detect is the communication method employed by Ethernet and Fast Ethernet.

Dynamic Host Control Protocol (DHCP)

Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

Extensible Authentication Protocol over LAN (EAPOL)

EAPOL is a client authentication protocol used by this switch to verify the network access rights for any device that is plugged into the switch. A user name and password is requested by the switch, and then passed to an authentication server (e.g., RADIUS) for verification. EAPOL is implemented as part of the IEEE 802.1x Port Authentication standard.

End Station

A workstation, server, or other device that does not act as a network interconnection.

Ethernet

A network communication system developed and standardized by DEC, Intel, and Xerox, using baseband transmission, CSMA/CD access, logical bus topology, and coaxial cable. The successor IEEE 802.3 standard provides for integration into the OSI model and extends the physical layer and media with repeaters and implementations that operate on fiber, thin coax and twisted-pair cable.

Fast Ethernet

A 100 Mbps network communication system based on Ethernet and the CSMA/CD access method.

Full Duplex

Transmission method that allows switch and network card to transmit and receive concurrently, effectively doubling the bandwidth of that link.

GARP VLAN Registration Protocol (GVRP)

Defines a way for switches to exchange VLAN information in order to register necessary VLAN members on ports along the Spanning Tree so that VLANs defined in each switch can work automatically over a Spanning Tree network.

Generic Attribute Registration Protocol (GARP)

GARP is a protocol that can be used by endstations and switches to register and propagate multicast group membership information in a switched environment so that multicast data frames are propagated only to those parts of a switched LAN containing registered endstations. Formerly called Group Address Registration Protocol.

Generic Multicast Registration Protocol (GMRP)

GMRP allows network devices to register endstations with multicast groups. GMRP requires that any participating network devices or endstations comply with the IEEE 802.1p standard.

Gigabit Ethernet

A 1000 Mbps network communication system based on Ethernet and the CSMA/CD access method.

Group Attribute Registration Protocol

See Generic Attribute Registration Protocol.

IEEE 802.1D

Specifies a general method for the operation of MAC bridges, including the Spanning Tree Protocol.

IEEE 802.1Q

VLAN Tagging—Defines Ethernet frame tags which carry VLAN information. It allows switches to assign endstations to different virtual

LANs, and defines a standard way for VLANs to communicate across switched networks.

IEEE 802.1p

An IEEE standard for providing quality of service (QoS) in Ethernet networks. The standard uses packet tags that define up to eight traffic classes and allows switches to transmit packets based on the tagged priority value.

IEEE 802.3

Defines carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications.

IEEE 802.3ab

Defines CSMA/CD access method and physical layer specifications for 1000BASE-T Fast Ethernet.

IEEE 802.3ac

Defines frame extensions for VLAN tagging.

IEEE 802.3u

Defines CSMA/CD access method and physical layer specifications for 100BASE-TX Fast Ethernet.

IEEE 802.3x

Defines Ethernet frame start/stop requests and timers used for flow control on full-duplex links.

IEEE 802.3z

Defines CSMA/CD access method and physical layer specifications for 1000BASE Gigabit Ethernet.

IEEE 802.1x

Port Authentication controls access to the switch ports by requiring users to first enter a user ID and password for authentication.

IGMP Snooping

Listening to IGMP Query and IGMP Report packets transferred between IP Multicast Routers and IP Multicast host groups to identify IP Multicast group members.

Internet Control Message Protocol (ICMP)

Commonly used to send echo messages (i.e., Ping) for monitoring purposes.

Internet Group Management Protocol (IGMP)

A protocol through which hosts can register with their local router for multicast services. If there is more than one multicast router on a given subnetwork, one of the routers is made the “querier” and assumes responsibility for keeping track of group membership.

In-Band Management

Management of the network from a station attached directly to the network.

IP Multicast Filtering

A process whereby this switch can pass multicast traffic along to participating hosts.

Layer 2

Data Link layer in the ISO 7-Layer Data Communications Protocol. This is related directly to the hardware interface for network devices and passes on traffic based on MAC addresses.

Link Aggregation

See Port Trunk.

Media Access Control (MAC)

A portion of the networking protocol that governs access to the transmission medium, facilitating the exchange of data between network nodes.

Management Information Base (MIB)

An acronym for Management Information Base. It is a set of database objects that contains information about a specific device.

Multicast Switching

A process whereby the switch filters incoming multicast frames for services for which no attached host has registered, or forwards them to all ports contained within the designated multicast VLAN group.

Out-of-Band Management

Management of the network from a station not attached to the network.

Port Authentication

See IEEE 802.1x

Port Mirroring

A method whereby data on a target port is mirrored to a monitor port for troubleshooting with a logic analyzer or RMON probe. This allows data on the target port to be studied unobstructively.

Port Trunk

Defines a network link aggregation and trunking method which specifies how to create a single high-speed logical link that combines several lower-speed physical links.

Private VLAN

Private VLANs segregate traffic into a non-broadcast domain. Traffic from a promiscuous port can pass between all ports that belong to the same primary VLAN. Traffic from a host port in a secondary VLAN can be forwarded to a promiscuous port in the associated primary VLAN or to other ports that belong to the same community VLAN.

Rate-Limit

This function allows the network manager to control the maximum rate for traffic transmitted or received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic

into or out of the network. Traffic that falls within the rate limit is transmitted, while packets that exceed the acceptable amount of traffic are dropped.

Remote Authentication Dial-in User Service (RADIUS)

RADIUS is a logon authentication protocol that uses software running on a central server to control access to RADIUS-compliant devices on the network.

Remote Monitoring (RMON)

RMON provides comprehensive network monitoring capabilities. It eliminates the polling required in standard SNMP, and can set alarms on a variety of traffic conditions, including specific error types.

Simple Network Management Protocol (SNMP)

The application protocol in the Internet suite of protocols which offers network management services.

Spanning Tree Protocol (STP)

A technology that checks your network for any loops. A loop can often occur in complicated or backup linked network systems. Spanning Tree detects and directs data along the shortest available path, maximizing the performance and efficiency of the network.

Telnet

Defines a remote communication facility for interfacing to a terminal device over TCP/IP.

Transmission Control Protocol/Internet Protocol (TCP/IP)

Protocol suite that includes TCP as the primary transport protocol, and IP as the network layer protocol.

Trivial File Transfer Protocol (TFTP)

A TCP/IP protocol commonly used for software downloads.

Virtual LAN (VLAN)

A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. A VLAN serves as a logical workgroup with no physical barriers, and allows users to share information and resources as though located on the same LAN.

XModem

A protocol used to transfer files between devices. Data is grouped in 128-byte blocks and error-corrected.

APPENDIX C

PIN ASSIGNMENTS

Console Port Pin Assignments

The DB-9 serial port on the switch's front panel is used to connect to the switch for out-of-band console configuration. The onboard menu-driven configuration program can be accessed from a terminal, or a PC running a terminal emulation program. The pin assignments used to connect to the serial port are provided in the following tables.

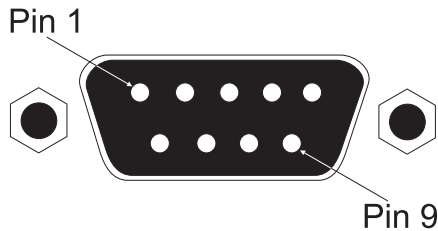


Figure C-1. DB-9 Console Port Pin Numbers

DB-9 Port Pin Assignments

| EIA Circuit | CCITT Signal | Description | Switch's DB9 DTE Pin # | PC DB9 DTE Pin # |
|-------------|--------------|-------------------------------|------------------------|------------------|
| BB | 104 | RxD (Received Data) | 2 | 2 |
| BA | 103 | TxD (Transmitted Data) | 3 | 3 |
| AB | 102 | SGND (Signal Ground) | 5 | 5 |

No other pins are used.

Console Port to 9-Pin DTE Port on PC

| Switch's 9-Pin Serial Port | Null Modem | PC's 9-Pin DTE Port |
|----------------------------|-----------------|---------------------|
| 2 RXD | <-----TXD ----- | 3 TXD |
| 3 TXD | -----RXD -----> | 2 RXD |
| 5 SGND | -----SGND ----- | 5 SGND |

No other pins are used.

Console Port to 25-Pin DTE Port on PC

| Switch's 9-Pin Serial Port | Null Modem | PC's 25-Pin DTE Port |
|----------------------------|-----------------|----------------------|
| 2 RXD | <-----TXD ----- | 2 TXD |
| 3 TXD | -----RXD -----> | 3 RXD |
| 5 SGND | -----SGND ----- | 7 SGND |

No other pins are used.

INDEX

A

address table 2-38

B

BOOTP 2-13

broadcast storm, threshold 2-34

C

Class of Service

 configuring 2-77

 queue mapping 2-77

community string 2-83

configuration settings, saving or
 restoring 2-22

console port

 pin assignments C-1

D

default settings 1-14

DHCP 2-13

dot1x

 commands 3-44

 configure 2-103

 default 3-46

downloading software 2-20

F

firmware upgrades 2-20

firmware version, displaying 2-28

H

hardware version, displaying 2-28

I

IGMP, configuring 2-86

ingress filtering 2-65

IP address

 BOOTP/DHCP service 2-13

 setting 2-11

L

log-in

 Web interface 2-2

login authentication

 RADIUS server 2-17

M

main menu 2-5

mirror port, configuring 2-37

multicast

 configuring 2-86

 router 2-89

P

passwords

 administrator setting 2-15

pin assignments

 25-pin DTE port C-2

 9-pin DTE port C-2

 console port C-1

port authentication commands 3-44

port priority, configuring 2-77

ports, configuring 2-30

private VLANs

 configuring 2-68

problems, troubleshooting A-1

R

RADIUS, logon authentication 2-17
rate limit configuration 2-98
restarting the system 2-24

S

serial port
 configuring 3-61, 3-68, 3-86
SNMP
 community string 2-83
 enabling traps 2-84
 trap manager 2-84
software downloads 2-20
software version, displaying 2-28
Spanning Tree Protocol 2-42
startup configuration file,
 creating 2-22
startup files
 displaying 2-20
 setting 2-20
statistics, switch 2-96
system software
 downloading from server 2-20
system, restart menu 2-24

T

trap manager 2-84
troubleshooting A-1
trunk, configuration 2-79

U

upgrading software 2-20
user password 2-15

V

VLANs, configuring 2-52

W

Web interface
 access requirements 2-1
 configuration buttons 2-3
 home page 2-3
 menu list 2-5
 panel display 2-4

FOR TECHNICAL SUPPORT, CALL:

From U.S.A. and Canada (24 hours a day, 7 days a week)

(800) SMC-4-YOU; (949) 679-8000; Fax: (949) 679-1481

From Europe (8:00 AM - 5:30 PM UK Time)

44 (0) 118 974 8700; Fax: 44 (0) 118 974 8701

INTERNET

E-mail addresses:

techsupport@smc.com

european.techsupport@smc-europe.com

support@smc-asia.com

Driver updates:

http://www.smc.com/index.cfm?action=tech_support_drivers_downloads

World Wide Web:

<http://www.smc.com>

<http://www.smc-europe.com>

<http://www.smc-asia.com>

FOR LITERATURE OR ADVERTISING RESPONSE, CALL:

| | | |
|----------------------|----------------------|-------------------------|
| U.S.A. and Canada: | (800) SMC-4-YOU; | Fax (949) 679-1481 |
| Spain: | 34-93-477-4935; | Fax 34-93-477-3774 |
| UK: | 44 (0) 118 974 8700; | Fax 44 (0) 118 974 8701 |
| France: | 33 (0) 41 38 32 32; | Fax 33 (0) 41 38 01 58 |
| Italy: | 39 02 739 12 33; | Fax 39 02 739 14 17 |
| Benelux: | 31 33 455 72 88; | Fax 31 33 455 73 30 |
| Central Europe: | 49 (0) 89 92861-0; | Fax 49 (0) 89 92861-230 |
| Switzerland: | 41 (0) 1 9409971; | Fax 41 (0) 1 9409972 |
| Nordic: | 46 (0) 868 70700; | Fax 46 (0) 887 62 62 |
| Northern Europe: | 44 (0) 118 974 8700; | Fax 44 (0) 118 974 8701 |
| Eastern Europe: | 34 -93-477-4920; | Fax 34 93 477 3774 |
| Sub Saharian Africa: | 27-11 314 1133; | Fax 27-11 314 9133 |
| North Africa: | 34 93 477 4920; | Fax 34 93 477 3774 |
| Russia: | 7 (095) 290 29 96; | Fax 7 (095) 290 29 96 |
| PRC: | 86-21-6485-9922; | Fax 86-21-6495-7924 |
| Taiwan: | 886-2-8797-8006; | Fax 886-2-8797-6288 |
| Asia Pacific: | (65) 238 6556; | Fax (65) 238 6466 |
| Korea: | 82-2-553-0860; | Fax 82-2-553-7202 |
| Japan: | 81-3-5645-5715; | Fax 81-3-5645-5716 |
| Australia: | 61-2-8875-7887; | Fax 61-2-8875-7777 |
| India: | 91 22 696 2790; | Fax 91 22 696 2794 |
| Middle East: | 97 14 299 4466 | Fax 97 14 299 4664 |
| Thailand: | 66 2 651 8733 | Fax 66 2 651 8737 |

If you are looking for further contact information, please visit www.smc.com,
www.smc-europe.com or www.smc-asia.com.

SMC[®]
Networks

38 Tesla

Irvine, CA 92618

Phone: (949) 679-8000

Model Number: SMC6724L2 F2.0.0.21

Pub.Number: 150200033600A E052003-R02